Table of Contents - Volume 1

Table of Contents - Volume 2

Background

During the 1994 Special Crime Session, the North Carolina General Assembly created the Criminal Justice Information Network Study Committee ("the Committee") to accomplish specific objectives regarding a plan for a statewide criminal justice information network. This legislation was enacted based on a recognition of the need for further coordination and cooperation between state and local agencies in establishing standards for sharing of criminal justice information. In November 1994, the Committee selected Price Waterhouse to assist them in fulfilling their mandate.

We began work in mid-December 1994 and delivered this report to the Committee in April 1995.

Our study focused on developing recommendations to promote the sharing of criminal justice information on a statewide basis between state and local agencies.

CJIN Study Objective

The following objective was developed and adopted by the Committee and the Price Waterhouse team. This objective best summarizes the principal vision and purpose for developing a statewide Criminal Justice Information Network.

"To identify alternatives for development of a statewide criminal justice information network that will enable a properly authorized user to readily access and effectively use information regardless of its location in national, state, or local databases."

Project Approach

The development of a plan for the creation of a criminal justice information network for North Carolina constitutes a high-level strategic planning project.

The Price Waterhouse CJIN team comprised senior-level consultants who possess in-depth strategic planning, technology, and organizational experience within the criminal justice environment.

A number of methods were employed to gather information, analyze information, and identify strategic opportunities from a substantial, diverse group of current and future criminal justice information users. These methods included personal interviews with more than 50 stakeholders statewide, six regional public hearings, 19 focus groups with six to 12 individuals attending each one, a national best practices survey of the other 49 states, an in-state survey of more than 1,000 criminal justice professionals, and sponsorship of three Open Public Events Network (OPEN/net) cable television call-in shows. More than 400 individuals within the state personally provided input to this study.

Summary of Findings

North Carolina's collection of criminal justice information systems is not designed to meet today's needs on a statewide scale.

Although the state is considered a leader in regards to certain independent agency information systems, (including participation by the State Bureau of Investigation in the FBI's National Fingerprint File, and implementation of a statewide court system by the Administrative Office of the Courts), there is a lack of integrated, and easily accessible criminal justice information across state and local agencies. This limits the efficiency and effectiveness of criminal justice professionals, and compromises the safety of both the public and law enforcement officers.

This independent approach to statewide systems development and data sharing is inadequate to support the current and future demand for integrated criminal justice information.

The following are the deficiencies that impede the effective integration and utilization of information. Our subsequent recommendations and strategies address these issues.

- *The elapsed time to positively identify persons entering the criminal justice system is unacceptable.*

  The current process of identification through fingerprints can take two weeks or more from initial fingerprinting of the offender until receipt of positive identification by the arresting agency. This process is hampered by the lack of livescan digitized fingerprinting technology at the fingerprint origination site as well as the lack of electronic access to a statewide database of digitized fingerprints. Upcoming IAFIS (Interstate Automated Fingerprint Identification System) standards mandate a two hour or less turnaround time for positive identification through fingerprints. Current North Carolina technology cannot meet these standards.

  The lack of a timely identification process is one of the most far-reaching problems affecting the availability and accuracy of individual information in all systems statewide. This situation has resulted in offenders who present false information upon arrest, being released before the discovery of an extensive criminal history, or unserved warrants.

- *A single, comprehensive source for a person's criminal history is not available in North Carolina.*

  Magistrates, district attorneys, investigators, field law enforcement officers, and other criminal justice professionals must search several separate criminal histories and manually match names and charges in order to compile a comprehensive history. Often, a complete search is not done or searches report inconsistencies in data between the systems. Mistakes are also made in correlating the information.

- *A single source of outstanding warrants does not exist.*

  An officer cannot query a single system to identify all outstanding warrants statewide. Although the State Bureau of Investigation's Division of Criminal Information (SBI / DCI) currently provides a statewide warrants database, it is not regularly used by many agencies, and the majority of outstanding warrants in the state are not

contained within this system. Local agencies resist the redundant entry of warrant information required to update all federal, state, and local databases.

A number of local law enforcement agencies maintain their own automated warrant systems. Separately, the clerks of the superior court enter warrant information into the Administrative Office of the Courts' (AOC) criminal system, while SBI / DCI and the National Crime Information Center (NCIC) are individually updated. Currently, the officer in the field does not know if a suspect has an outstanding warrant in the adjacent county or elsewhere in the state. The officer may not even know if there is an outstanding warrant in the same county.

- *Statewide, interagency, mobile voice and data communication is not available.*

  We have noted repeated frustration with the inability of most law enforcement / public safety agencies to communicate through incompatible mobile radios while participating in a joint response. In addition, there is a growing need for mobile data access for all law enforcement and public safety agencies, ranging from simple vehicle and driver's license checks, to full criminal history searches, photo imaging, and remote entry of incident, arrest, accident, and citation information from the field. Due to the lack of statewide standards and definitions, considerable funds are being spent in an effort to address this problem in an uncoordinated fashion. The result is multiple pockets of expensive implementations throughout the state, based on differing technology, without the ability to interconnect adjoining sites.

- *Excessive redundant data entry exists within state and local agencies.*

  We have found redundant entry of data by each criminal justice agency as the offender moves through each step of the criminal justice system. The same offender information is currently entered and reentered into computers, typewritten, and handwritten from five to 10 times during an offender's journey from arrest through release. The arresting officer completes the arrest and incident report. The magistrate completes the warrant or magistrate's order and commitment / release order. The sheriff books the offender into jail. The clerk creates the case file information within the AOC system. The district attorney may create separate case records. The

Department of Correction (DOC) creates a prison file. Probation and parole officers create the supervision file. The ramifications of this redundancy are clear:

1. Wasted staff time that results in ineffective and inefficient use of already stretched state and local resources.

2. Delay in making the information available to the critical users of the various state and local systems.

3. Reduction in the accuracy of information each time data is reentered.

4. Elongation of the time required for the offender to move through the criminal justice system, which reinforces the public's perception of inefficient bureaucracy.

5. Limits in the quantity of data captured for statewide use.

Summary of Recommendations

Based on our findings, we recommend several steps to create and integrate a statewide Criminal Justice Information Network.

- ✓ Establish a Criminal Justice Information Network governance board to create, promote, and enforce policies and standards.
- ✓ Adopt system architecture standards to facilitate movement of data between state and local systems.
- ✓ Establish data standards for sharing information, including common definitions, code structures, and formats.
- ✓ Implement livescan digitized fingerprint systems and Automated Fingerprint Identification System (AFIS) technology to accomplish positive fingerprint identification within two hours of arrest.
- ✓ Implement a magistrate system statewide to streamline the process of warrant and case creation.
- ✓ Implement a statewide, fingerprint-based criminal history that includes *all* arrests and dispositions.
- ✓ Build a statewide identification index which includes information from all local and state agencies, as well as the necessary linkages to federal justice agencies.
- ✓ Establish standards for, and implement a mobile voice and data communication network that allows state and local law enforcement and public safety agencies to communicate with each other, regardless of location in the state.
- ✓ Leverage the potential of the North Carolina Information Highway (NCIH) as a feasible CJIN building block.

Specific projects have been identified and described to address our findings and recommendations. These projects are grouped into the following categories:

Management: Those activities to be undertaken to resolve start-up and ongoing governance issues.

Infrastructure: Those projects necessary to create a cohesive and consistent architecture so that information can be entered and shared throughout the network. These include:

1. Data Sharing Standards Development
2. CJIN Security
3. TCP/IP Communication Standard
4. End-User Technology Upgrade
5. Statewide Mobile Voice and Data

Applications: Those projects necessary to create or integrate application software and data to provide robust functionality to users across the network. Our focus on application software has been on those projects that promote the sharing of criminal justice information on a statewide basis between state and local agencies. We addressed processes that contained bottlenecks or redundancies in the current system. These applications include:

6. Statewide Automated Fingerprint Identification System
7. Statewide Magistrate System
8. Statewide Identification Index
9. Statewide Criminal History Repository
10. Statewide Warrant Repository
11. Courtroom Automation
12. Juvenile Records Automation

Further, we have presented our suggested projects in a hierarchical manner that recognizes key dependencies. For instance, prior to expanding the criminal case history database, it is necessary to establish a consistent and unique statewide personal identifier, and use data standards so that information can be shared with law enforcement, courts, and corrections. The organization of the recommended projects is depicted in Figure ES-1.

The combination of these projects will tie together current information and create new processes and databases to support an integrated criminal justice information network. Our recommendations focus on enterprise-wide issues on a vertical (between state and local agencies) and a horizontal (between law enforcement, courts and corrections) basis. The scope of our study did not include intra-agency concerns except to the extent that an enterprise-wide need existed. As a result, our recommendations are not intended to impact the information plans specific and internal to an individual state or local agency, where no external requirements were noted.

Each of the projects and strategies we have recommended will result in significant benefits on their own merits. However, commitment to the overall plan of implementation is key to realizing the maximum return on the state's CJIN investment. Overall safety and effectiveness can be dramatically improved through the adoption of the long-term vision and strategy. Similar to the blocks in the foundation of a building, the elimination of cornerstones, construction out of sequence, or acceptance of low grade products will substantially weaken the entire structure.

Summary of Estimated Costs for Recommended CJIN Projects

The following tables provide a summary of the estimated initial and ongoing annual costs for the Governance Board and each project we have recommended. We have provided these estimates as an indication of magnitude for each of the projects. Subsequent budget estimates should be based on prevailing market prices at the time the work is to be undertaken and adjusted by the final scope of the work.

Project Costs ($millions)	*Initial Costs*	*Annual Costs*
Governance Board	$0.4	$0.7
1. Data Sharing Standards Development	$2.1	$0.8
2. CJIN Security	$0.9	$0.1
3. TCP/IP	$4.6	$13.9
4. End-User Technology Upgrade	$21.2	$1.9
5. Statewide Mobile Voice and Data (separate table)	***	***
6. Statewide Automated Fingerprint Identification System	$22.4	$2.6
7. Statewide Magistrate System	$5.0	$1.3
8. Statewide Identification Index	$6.7	$1.4
9. Statewide Criminal History Repository	$4.8	$1.0
10. Statewide Warrant Repository	$4.2	$1.1
11. Courtroom Automation	$10.1	$2.0
12. Juvenile Records Automation	$8.8	$1.1
Totals	**$91.2**	**$27.9**

Estimated Statewide Mobile Voice and Data Costs

The table below estimates state costs only and does not reflect local agency investments for portables, in-building coverage, and roaming stock.

Statewide Mobile Voice and Data Project - Projected State Cost ($Millions)

Task\Year	1	2	3	4	5	6	7	8	9	10	Total
MODAP Pilot	0.5	0.5	0.5								1.5
Frequency Study	0.5										0.5
County Planning	1.0	1.5	1.0	1.0	0.5	0.5	0.5	0.5	0.5	0.5	7.5
Implementation				35.0	35.0	35.0	34.0	34.0	34.0	34.0	241.0
Maintenance					3.5	6.0	8.5	13.5	16.0	18.5	66.0
Total ($millions)	**$2.0**	**$2.0**	**$1.5**	**$36.0**	**$39.0**	**$41.5**	**$43.0**	**$48.0**	**$50.5**	**$53.0**	**$316.5**

Complete project descriptions, estimated costs detail, and costing assumptions are contained within Section VI - Overview of CJIN Projects, while Section VII - Implementation Alternatives provides a discussion of the three alternatives to CJIN project implementation.

Commitment to Action

The General Assembly, together with the Executive and Judicial branches, must accept that support for the CJIN enterprise is a long-term capital investment. In addition to required start-up funds and project development monies, there also must be a long-term commitment to a new way of doing business. A primary consideration must be the realization that state and local agencies already are spending considerable funds on the issues addressed in our recommendations.

The option, therefore, is not whether money will be spent on the criminal justice system, but whether the expenditures will be targeted, coordinated, and designed for the maximum benefit of users statewide.

For these reasons in particular, it is critical that the CJIN Governance Board and initial phases of the infrastructure projects are approved, established and funded by the General Assembly as promptly as possible. If this is not accomplished in the 1995 legislative session, there will be no visible leadership to direct the development of the recommendations made in this report and to serve as an advocate for the CJIN enterprise. In addition, a delay will cause some state agencies and local jurisdictions to further commit their limited funds to the development and enhancement of systems that do not support an integrated network.

Further delays add to the fragmentation of the system, and make future connections even more difficult. And finally, a delay in addressing this issue would send a message to the general public that the state is not serious about moving forward on this issue despite the high level of consensus of users across the state as represented in our findings and recommendations.

Introduction

This report presents the results of a study conducted by Price Waterhouse LLP ("Price Waterhouse") on the development of a statewide Criminal Justice Information Network (CJIN) for North Carolina.

During the 1994 Special Crime Session, the North Carolina General Assembly created the Criminal Justice Information Network Study Committee (“the Committee”) to accomplish specific objectives regarding a plan for a statewide criminal justice information network. Through a competitive procurement process, the Committee selected Price Waterhouse, in November 1994, to assist them in fulfilling their mandate.

Price Waterhouse began work in mid-December 1994 and delivered this report to the Committee in April 1995.

Our study focused on developing recommendations to promote the sharing of criminal justice information on a statewide basis between state and local agencies. The scope of the project did not encompass recommendations regarding the internal information needs of any one particular state or local agency that was not related to the overall CJIN objective.

This introduction provides an overview of the following:

- CJIN Study Committee Members
- CJIN Study Objective, Goals, and Critical Success Factors
- Project Approach
- Summary of Report Sections

CJIN Study Committee Members

The Criminal Justice Information Network Study Committee was created to provide a plan for a statewide, integrated criminal justice information network as mandated by the General Assembly. The Committee includes nine members appointed by Governor James B. Hunt, their proxies, and four members from the IRMC appointed by the IRMC Chairman the Honorable Rufus L. Edmisten, and their proxies, as listed below. The project manager, selected by the Committee, is Mr. Richard C. Little, who is on a leave-of-absence from the Administrative Office of the Courts.

CJIN Study Committee Members	Proxy
Mr. Ronald P. "Ron" Hawley (Co-Chair) Assistant Director Division of Criminal Information State Bureau of Investigation	Mr. George Bakolia Data Processing Manager Division of Criminal Information State Bureau of Investigation
Mr. John C. Wyatt (Co-Chair) Executive Director Mecklenburg County Criminal Justice Commission	No proxy designated
Mr. William C. "Bill" Clontz Director of Information Services New Hanover County	No proxy designated
Mr. James C. "Jim" Drennan Director Administrative Office of the Courts	Mr. Fran Taillefer Administrator Information Services Division Administrative Office of the Courts

CJIN Study Committee Members	Proxy
The Honorable Rufus L. Edmisten Secretary of State	Mr. Glenn Wells Special Deputy Secretary of State's Office
Ms. LaVee Hamer Legal Counsel Department of Correction	Mr. Bob Brinson Director, Management Information Systems Department of Correction
Chief Chester Hill Goldsboro Police Department	Major Floyd Hobbs Goldsboro Police Department
Mr. Albert "Al" Little Director of Information Systems Department of Crime Control and Public Safety	Lt. Fred Davis State Highway Patrol
The Honorable Frank McGuirt Sheriff of Union County	Sgt. Ben Bailey Union County Sheriff Department

IRMC CJIN Study Committee Members	Proxy
Ms. Janet Smith (Chair) Senior Vice President Group Executive Retail Support Operations Wachovia Bank and Trust Company	No proxy designated
The Honorable James E. Long Commissioner of Insurance	Mr. John Coan Director of Information Systems Department of Insurance
The Honorable Ralph Campbell, Jr. State Auditor	Dr. Lenox "Lenny" Superville Director of Information Systems Office of the State Auditor
Colonel Robert A. Barefoot Commander of the Highway Patrol	Lt. Fred Davis State Highway Patrol

CJIN Study Objective, Goals, and Critical Success Factors

CJIN Objective

The following objective was developed and adopted by the Committee and the Price Waterhouse team. This objective best summarizes the principal vision and purpose for developing a statewide Criminal Justice Information Network.

"To identify alternatives for development of a statewide criminal justice information network that will enable a properly authorized user to readily access and effectively use information regardless of its location in national, state, or local databases."

In order to best describe the intent and scope of the CJIN objective, each key phrase of this objective and its effect on our report has been further described:

"To identify alternatives..."

Although there is one vision for the CJIN objective and goals, the project team identified three alternative implementation strategies to achieve that vision. Our report summarizes and presents these implementation and cost alternatives for the development of a criminal justice information network for the state. Each of the alternatives provides a different approach to the costs and implementation timing issues. Although the same critical projects are recommended with each alternative, variations in timing provide the state of North Carolina flexibility in achieving implementation objectives.

"... for development of a statewide criminal justice information network ..."

Our report provides the blueprint for an envisioned network of hardware, software, and organizations that will facilitate the sharing and exchange of information among local and state criminal justice agencies and private citizens. CJIN will demand continuing strategic investment in a variety of projects that address specific issues while furthering the enterprise-wide, long-term CJIN goals.

"... that will enable a properly authorized user ..."

The creation of a more accessible and open criminal justice information network will demand security that provides both a high level of protection as well as flexibility. CJIN must ensure secure operation against the growing number of "hackers" and curious users who will increasingly test security through the open communication, hardware, and software standards that CJIN will necessarily employ. Conversely, the CJIN security must not present authorized users with undue and cumbersome restrictions, which prevent them from seamless and effortless navigation of existing and future CJIN systems, to update or obtain the requested information.

"... to readily access and effectively use information ..."

Our plan and the projects presented, provide for a CJIN that will permit users to view or update information in a timely, straightforward, and intuitive manner. Our report documents that much of the information needed by users of the criminal justice system already exists in one system or another. What does not exist, however, is the capability for a user to access this information in a reasonable amount of time, with a reasonable effort, and in a consistent, understandable form. Our recommendations promote the use of the North Carolina Information Highway (NCIH) as one option, along with a variety of other technologies, to facilitate this sharing.

"... regardless of its location in national, state, or local databases."

Our recommendations address the requirements for access to and update of information that resides in local, state, and national databases. The goal for CJIN is to present cogent information without the user requiring knowledge of the location of the information.

CJIN Goals

The goals adopted by the CJIN Study Committee in support of the overall objective are based on the enabling legislation. Our report addresses each goal as follows:

1. *Facilitate collection and dissemination of information. Data should be:*
   - *Entered once and whenever possible used thereafter throughout the criminal justice system.*
   - *Accurate, reliable, and timely.*
   - *Accessible in a meaningful, relevant, and understandable form, when and where needed.*

   As an example, our project recommendations include implementation of a statewide magistrate system and automation of the criminal courtroom functions. These projects will significantly reduce redundant entry of data and will provide information with greater accuracy and timeliness.

2. *Create a single, standard, personal identifier that links incidents, arrests, court cases, dispositions, inmates, treatments, victims, custody status, and release data.*

   We recommend adoption of the State Identification Number (SID) as the single, standard, statewide personal identifier. Implementation of livescan (digitized fingerprinting systems) and AFIS (Automated Fingerprint Identification System) technology will provide near real-time offender identification. Implementation of a Statewide Identification Index (SII) based on the SID will link together all local and state criminal justice information for a particular individual.

3. *Establish common, uniform definitions and code structures for such items as offenses, incidents, and cases, as well as common data definitions.*

   Our Data Sharing Standards Development Project (Section VI.1) recommendation provides a step-by-step guide for the development of a statewide data dictionary. Based on our nationwide best practices survey, this project

has been substantiated as the crucial first step in establishing uniform criminal justice definitions and standards among local and state criminal justice agencies.

4. *Provide for adequate security, privacy, and public access, including authorization, authentication, and encryption where necessary.*

   The CJIN Technical Strategy (Section V) provides an analysis and recommendation for implementing a security plan that will address privacy and public access needs. In addition, the CJIN Security Project (Section VI.2) discusses the details of the first step to implementing this security within existing systems and applications.

5. *Provide for flexibility for evolution in meeting the ever changing local, state, and federal needs.*

   The CJIN Technical Strategy section recommends a migration to open systems standards statewide for communications, hardware, databases, and application development consistent with Information Resource Management Commission (IRMC) standards. This step will provide CJIN with the technical flexibility to more easily adapt to changes in local, state, and federal needs. The CJIN Governance Strategy section provides for continued monitoring and updating of data sharing standards to provide a consistent base among systems for quickly reacting to changes in needs at all levels of government.

6. *Offer measurements for evaluation and accountability for gauging performance - this will include operations, membership, data quality and accuracy, and cost.*

   The CJIN Governance Strategy section of our report discusses one of the key functions of the CJIN governance group - measures of effectiveness. The Data Sharing Standards Development Project section includes recommendations for data quality audits.

7. Provide for use of existing systems, if appropriate, at the state and local levels. Consider a path for migrating to common statewide architectural standards if necessary.

The CJIN Technical Strategy section includes recommendations on a common statewide system architecture that leverages the existing systems while providing future adherence to open standards. The TCP / IP Project (Section VI.3), End-User Technology Upgrade Project (Section VI.4), and Data Sharing Standards Development Project (Section VI.1) leverage current hardware and software systems while providing an approach for moving to common standards. In addition, use of the NCIH will facilitate the connection of disparate systems.

CJIN Critical Success Factors

Critical success factors are those few things that must be done well to achieve the CJIN objective and goals. Critical success factors play a significant role in the development of a strategic plan as they provide the key linkage between North Carolina criminal justice system's business needs and its information system's strategy. Critical success factors focus attention on the high payoff areas, help build consensus, and prioritize projects.

Below is a list of the factors we identified as critical to the success of CJIN, and a summary of steps taken within the course of this study to ensure adherence to these critical success factors.

1. Search beyond present capabilities - set high standards and challenging expectations.

Our recommendations provide the blueprint for criminal justice integration throughout the state over the next five years. The strategies and projects selected were chosen for their ability to provide significant gains in effectiveness and efficiency. The plan presented is aggressive but feasible.

2. Obtain local acceptance of the study and public support of its recommendations.

At every step of the CJIN Study process, care has been taken to solicit the needs and opinions of criminal justice professionals at the state and local levels. Each recommendation has been presented to the Committee in three

separate work-in-progress documents. Follow-up interviews were conducted with key CJIN stakeholders at the executive levels of government to provide specific assessments of our recommendations. Focus group attendees were provided with up-to-date information on the findings and potential recommended solutions.

3. Create a responsive organizational structure for conducting the study:

- *Include primary participants*
- *Allow for appropriate review and approvals*
- *Facilitate performance of the study*
- *Coordinate with the IRMC*

As noted previously, extensive research was conducted with all primary participants and multiple checkpoints provided for formal review and approval. Four members from the Information Resource Management Commission and their proxies were appointed by IRMC Chairman and CJIN Study Committee member, the Honorable Rufus L. Edmisten, Secretary of State. These members were: Janet Smith, Senior Vice President, Wachovia Bank and Trust Company; the Honorable James L. Long, Commissioner of Insurance (John Coan, proxy); the Honorable Ralph A. Campbell, Junior, State Auditor (Dr. Lenny Superville, proxy); and Colonel Robert A. Barefoot, Commander of the Highway Patrol (Lt. Fred Davis, proxy). These individuals were interviewed regarding their vision for CJIN; they were invited to all CJIN Committee meetings; and they received copies of all information that was distributed at CJIN Study Committee meetings and to the Committee members. In addition, Nick Barnet from the Office of the State Controller (OSC) / Information Resource Management Division (IRM), participated in many of the focus groups and a best practices visit to the state of Maryland, providing the Price Waterhouse team with ongoing feedback, comments, and critiques.

4. Organize the technology within IRMC standards where possible.

The technology standards we recommend adhere to the IRMC technology standards where they exist.

5. Provide for education and awareness of all stakeholders.

The Price Waterhouse team interviewed more than 50 individuals within state and local government and private industry, conducted six public regional hearings, and facilitated 19 focus groups. This effort was designed to both solicit information needs from, and provide education and awareness to CJIN stakeholders. More than 400 individuals within the state personally contributed to the CJIN Study.

6. *Present practical and reasonable recommendations. Provide for a balanced mix of near-term deliverables and long-range, high-return deliverables.*

   In addition to providing long-term strategies and projects, we have included short-term recommendations for the improvement of systems and business processes. Examples include the immediate distribution of livescan fingerprint devices to local agencies and the creation of centralized warrant repositories in each county.

7. *Evaluate, judge, and reach conclusions using the best available information, knowledge, and experience within the time frames established by the General Assembly.*

   Conclusions in the form of our findings and recommendations were completed by the established dates. Due to delays in the state awarding the CJIN Study contract to Price Waterhouse, the original timeframe for completion of this effort was shortened to three months from the planned five months. In order to accommodate this new timeline and provide the final report for presentation to the General Assembly in April 1995, the following steps were taken: 1) agreement on specific limits for the scope of juvenile justice to include delinquency but not dependency; 2) conducted the first few weeks of focus groups immediately, resulting in tight scheduling for some attendees; 3) increased Price Waterhouse staffing and included additional specialized consultants for specific areas; and 4) focused on the critical elements as presented in the General Assembly enabling legislation.

Project Approach

The recommendations for the creation of a criminal justice information network for North Carolina constitute a high-level planning project. Two proven Price Waterhouse methodologies have been employed as a framework for this study: Strategic Information Systems Planning (SISP) and Change Integration (CI).

SISP is the process of developing a plan for the use of information systems within an organization which is both cost-effective and aligned with the prioritized managed and operational needs of the organization. SISP leads to the identification of strategic initiatives, either new or already underway, which can be aided by application systems, technology, and management. The SISP methodology includes four stages: 1) determine business and information needs; 2) define information systems targets; 3) define and select information systems strategy; and 4) develop implementation plans.

The CI methodology was developed to guide organizations through the tasks and activities needed to achieve successful enterprise-wide change which is integral to the adaption of technology. The CI methodology includes four stages: 1) Evaluate; 2) Envision; 3) Empower; and 4) Excel. This study utilized the Evaluate and Envision phases of CI, which includes identification of change drivers, validation of mission, assessment of current environment and implementation of new processes, systems, culture, and technologies to achieve change. The combination of defining the current "as is" environment and envisioning the "to-be" environment provides a structured approach to manage change.

The Price Waterhouse CJIN team comprised senior-level consultants who possess in-depth strategic planning, technology, and organizational experience within the criminal justice environment.

A number of methods were employed to gather information, analyze information, and identify strategic opportunities from a substantial, diverse group of current and future CJIN users. These methods included personal stakeholder interviews, regional public hearings, focus groups, a national survey, an in-state survey, and three Open Public Events Network (OPEN/net) cable television call-in shows.

Stakeholder Interviews

The Price Waterhouse team conducted extensive interviews and follow-up interviews with a broad range of more than 50 stakeholders. All Committee members and / or proxies were interviewed at least once in order to understand their vision of CJIN, and their opinions on project priorities and strategies for success within their particular areas of expertise. Interviews were also conducted with certain Council of State officials, directors and key managers within state agencies, sheriffs, judges, district attorneys, clerks of the superior court staff, magistrates, county commissioners,

information systems managers, and analysts. A listing of interviewees and a discussion of the interview process are provided in Volume 2, Section E - Stakeholder Interviews.

Regional Public Hearings

To solicit input, generate awareness, and obtain local support from individuals across the state, Price Waterhouse and the CJIN Study Committee facilitated six regional public hearings in the following cities: Asheville, Charlotte, Edenton, Fayetteville, Kinston, and Winston-Salem. An invitation to these forums was extended to more than 4,500 criminal justice professionals across the state. In addition, notification of the hearings was distributed on the interagency E-mail networks of the State Bureau of Investigation's (SBI) Division of Criminal Information (DCI), the Administrative Office of the Courts (AOC), and the State Highway Patrol (SHP). A notice of the hearing was also sent to each local area newspaper.

More than 150 individuals representing courts, law enforcement, corrections, and community action groups attended one or more of the six public hearings. Further details regarding each public hearing and the principal issues and comments that were expressed are presented in Volume 2, Section B - Regional Public Hearings.

Focus Groups and Facilitated Sessions

A total of 19 focus groups and facilitated sessions were conducted during the three-month study period. The sessions examined the development of a criminal justice information network from a variety of perspectives and focused on specific portions of the CJIN. The focus groups generally lasted from four to six hours and included six to 14 participants.

There were three focus groups that dealt specifically with the plan for a statewide integrated wireless communication system for law enforcement. Four "horizontal" focus groups examined the current and future information needs from the Administrative Office of the Courts (AOC), Department of Correction (DOC), State Bureau of Investigation's

Division of Criminal Information (SBI / DCI), and the Division of Motor Vehicles (DMV) through the eyes of law enforcement, courts, and corrections users of all four state systems. Five "technical" focus groups reviewed the interfaces between the current criminal justice systems and discussed alternatives for the CJIN network architecture.

Three "vertical" sessions focused on the current and future needs within federal, state, and local law enforcement, corrections, and courts. There was a specific focus group to identify technical and business process solutions for implementation of a CJIN statewide personal identifier, and another focus group solicited information and ideas from six jurisdictions who have implemented all or part of an integrated criminal justice information system on the local level. One group examined the specific issues related to juvenile criminal justice, while another session met with sheriffs and police chiefs to better understand their perspective and needs.

Below is a listing of the specific sessions conducted. The minutes of each focus group are presented in Volume 2, Section A - Facilitated Sessions and Focus Groups.

Wireless Communications	Horizontal User Groups	Vertical User Groups
Mobile Voice and Data	Users of AOC Information	Correction
Mobile Voice	Users of DOC Information	Courts
Mobile Data	Users of DCI Information	Law Enforcement
	Users of DMV Information	

Technical Groups	Specific Topics
AOC / DCI Interface	Individual Statewide Identifier
AOC / DOC Interface	Local Integrated CJIS
DOC / DCI Interfaces	Juvenile Automation
AOC / DMV Interfaces	Sheriff / Police Chief Perspective
Network Architecture	

National Survey

Using information from sources such as the National Center for State Courts, SEARCH Group, and the American Jail Association as a starting point, and based on the team's personal experiences in almost every state, Price Waterhouse conducted a national best practices survey of states from which to collect information about integrated, automated criminal justice systems. There was a lack of readily accessible and accurate information about existing efforts in this important area and the survey method provided the most relevant information to the CJIN project. The purposes of the national survey were to:

- Identify the extent to which statewide criminal justice information networks exist and meet user needs in the other 49 states.

- Examine states with experiences most applicable to the CJIN Study for best practices that could be applied to North Carolina.

A complete discussion of the survey results is presented in Volume 2, Section C - National Survey.

In-State Survey

The in-state survey provided a unique opportunity to solicit information from approximately 1,100 state and local criminal justice professionals throughout North Carolina. A considerable amount of research on county and city systems had previously been compiled by Nick Barnet (OSC / IRM), which was used as a starting point. Our survey was a mechanism to both collect initial data and to validate information collected in other forums. The purposes of the survey were to determine the:

- Degree of satisfaction that system users have with existing state and local criminal justice information systems in North Carolina.
- Information needs of state and local criminal justice agencies in North Carolina.
- Degree to which technology exists, or would be useful to agencies where currently not available.

Please see Volume 2, Section D - In-State Survey for a complete listing of the survey results.

Summary of Report Sections

The CJIN Study Report is organized as follows:

Executive Summary

The Executive Summary provides a brief, high-level overview of the Criminal Justice Information Network Study Committee Report background, approach, findings, and recommendations.

Volume 1

I. Introduction

The introduction provides background on the CJIN Study and discusses the objective, goals and critical success factors, the project approach, and this summary of report sections.

II. Current Business Environment

This section provides documentation on the business environment of the current criminal justice information system.

III. Current Information Systems Environment

This section includes documentation on the information systems environment of the current criminal justice information system.

IV. Organizational Strategy

Recommended organizational strategies for CJIN include a discussion of the proposed CJIN Governance Board and Organizational Constraints.

V. Technical Strategy

Recommended technical strategies and standards for CJIN include data management standards, system architecture, security and advanced technologies.

VI. Project Strategy

This section presents the key projects which will support the objective and goals of the Criminal Justice Information Network. Each project reviews the current situation, the need for change, and identifies the recommended solution, including approach, business process changes, technology, and costs.

VII. Implementation Alternatives

Three CJIN cost and implementation alternatives are summarized in this section.

Volume 2

A. Facilitated Sessions and Focus Groups

This section describes the approach used and a summary of each facilitated session / focus group, including an attendance list, agenda, and documentation of issues and conclusions.

B. Regional Public Hearings

A description of the six regional public hearings is provided along with the approach used, objectives, and methods of promotion. A summary of each public hearing, including the number of persons attending, and key issues, is also included.

C. National Survey

This section describes the national survey and includes a review of the methodology used, a description of the survey document, and a summary of the results.

D. In-State Survey

This section describes the North Carolina in-state survey and includes a review of the approach, a description of the survey document, and a listing of the results.

E. Stakeholder Interviews

Stakeholder interviews are documented and a description of the approach, list of interviewees, questions and format, and a summary of information obtained is provided.

F. Definition of Terms

A glossary of terms and abbreviations that are used within the report is presented.

G. Reference Materials

A listing of all reference materials that were reviewed in preparing this report is provided.

H. Legislative Issues

Included in this section is an initial listing of selected statutes that bear on the projects recommended by this study.

I. Advanced Technologies

Advanced technologies and their current and future use within CJIN is discussed within this section.

Current Business Environment

A high-level understanding of the criminal justice "business" environment is necessary to develop a targeted and useful strategic plan. This section presents a review of the current North Carolina criminal justice information system "business" environment and includes the following components:

- Enterprise overview and process
- Missions and critical success factors
- Customers and stakeholders
- Change driver analysis

Enterprise Overview and Process

Our approach to this study involves treating CJIN as an integrated enterprise model. The purpose in viewing CJIN as an "enterprise" in its own right is to show the symbiotic relationships among criminal justice information users at the state and local levels, and across the various branches of government.

The primary organizations that produce and use criminal justice information within the state include:

- Local law enforcement agencies
- Administrative Office of the Courts
- Department of Correction
- State Bureau of Investigation / Division of Criminal Information
- State Highway Patrol
- Department of Transportation / Division of Motor Vehicles
- Department of Human Resources / Division of Youth Services

Figure II-1 depicts a high-level enterprise overview of current criminal justice information users from an organizational perspective. A discussion of the missions and critical success factors for each of the organizations depicted can be found later in this section. The diagram in Figure II-1 illustrates the dispersion of criminal justice users across agencies, levels, and branches. The current criminal justice information "system" is actually a collection of fragmented, automated, and manual, processes administered by organizations and units with missions and critical success factors that do not necessarily encourage cooperation across the criminal justice enterprise. The institutional structure, and the legal and political obstacles that have developed around it, have exacerbated difficulties with sharing information efficiently between organizations.

Within each of these organizations, at various levels, are numerous individuals whose information needs are driven by their roles and responsibilities and are dependent on the information systems and sources they can access. The key players in the criminal justice information arena include:

- Judges
- Clerks of the Superior Court (Clerk)
- District attorneys
- Public defenders
- Magistrates
- Juvenile court counselors
- State troopers
- AOC personnel
- Police officers
- SBI agents
- Sheriff deputies
- Prison and jail administrators
- Probation and parole officers
- Local social service agencies

An analysis of primary CJIN customers and stakeholders is found later in this section.

Figure II-2 is a representation of the criminal justice process: from local law enforcement's involvement with crime prevention to an offender's release from the Department of Correction's oversight and responsibility. Many different state and local organizations play a role in this process. Although this picture presents the criminal justice process as linear, in fact, many of the activities during the course of this process take place in a nonlinear fashion. The parallel processes increase the importance for each organization to produce and use timely and accurate information.

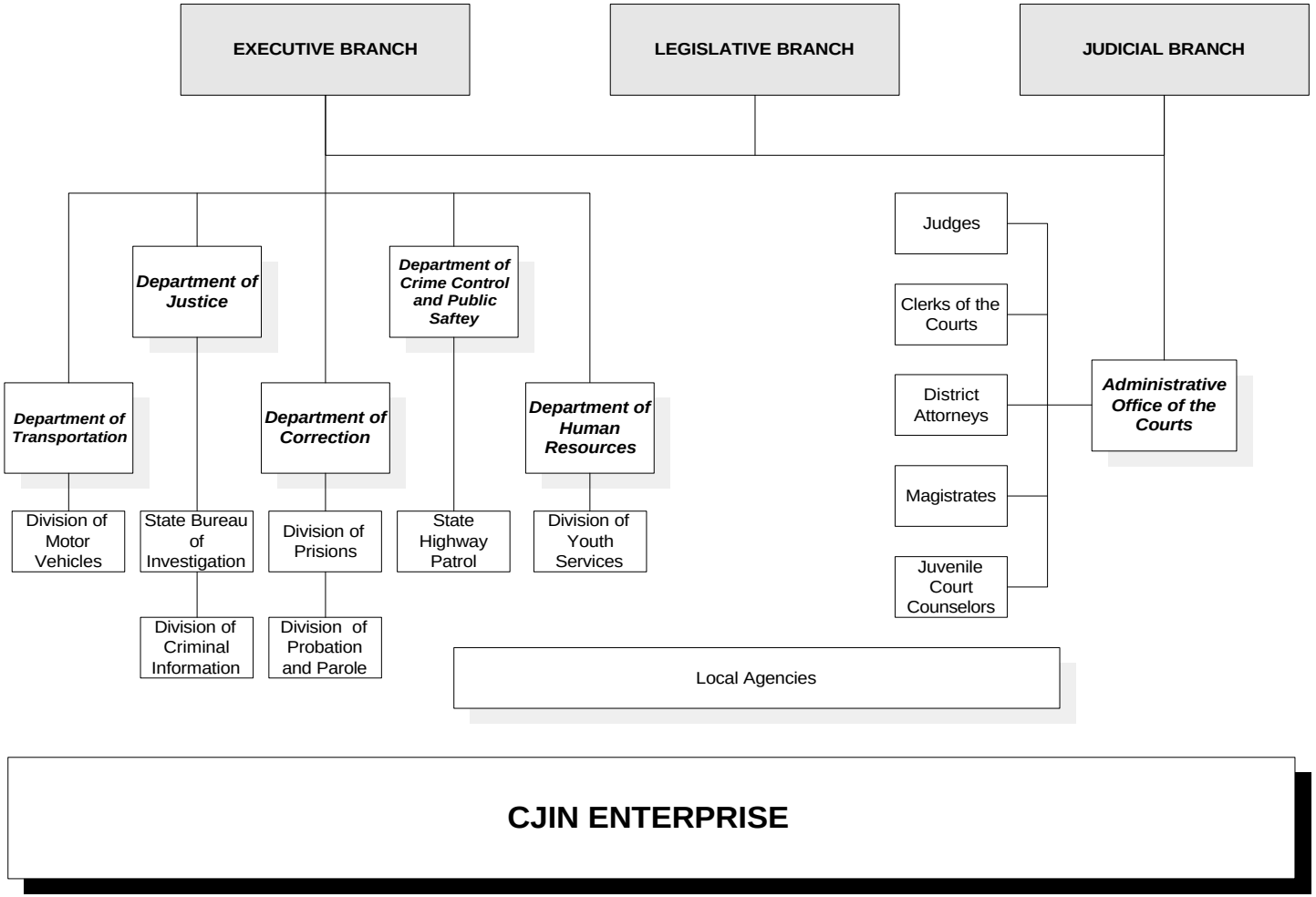

EXECUTIVE BRANCH
LEGISLATIVE BRANCH
JUDICIAL BRANCH
Department of Justice
Department of Crime Control and Public Saftey
Department of Transportation
Department of Correction
Department of Human Resources
Judges
Clerks of the Courts
District Attorneys
Magistrates
Juvenile Court Counselors
Administrative Office of the Courts
Division of Motor Vehicles
State Bureau of Investigation
Division of Prisions
State Highway Patrol
Division of Youth Services
Division of Criminal Information
Division of Probation and Parole
Local Agencies
CJIN ENTERPRISE

Figure II-1

Current Assessment

Even though total system integration, across all criminal justice agencies, is far from a reality in the State, North Carolina is considered a leader among other states with regard to independent agency information systems and cross-agency cooperative initiatives. For example, North Carolina is one of only three states currently participating in the FBI's Interstate Identification Index, National Fingerprint File (NFF) project. The goal of NFF is to eventually eliminate the need for duplicate information repositories at the state and federal level. In addition, the AOC operates one of the nation's statewide court information systems. There are numerous other examples of agencies within the state that are cooperating together while planning for or implementing state-of-the-art information systems.

However, criminal justice information systems are geared to meet the requirements of the sponsoring agency, and built with agency specific budgets. The usefulness of a particular system's data or functions to another agency or jurisdiction is typically of secondary or tertiary focus and importance.

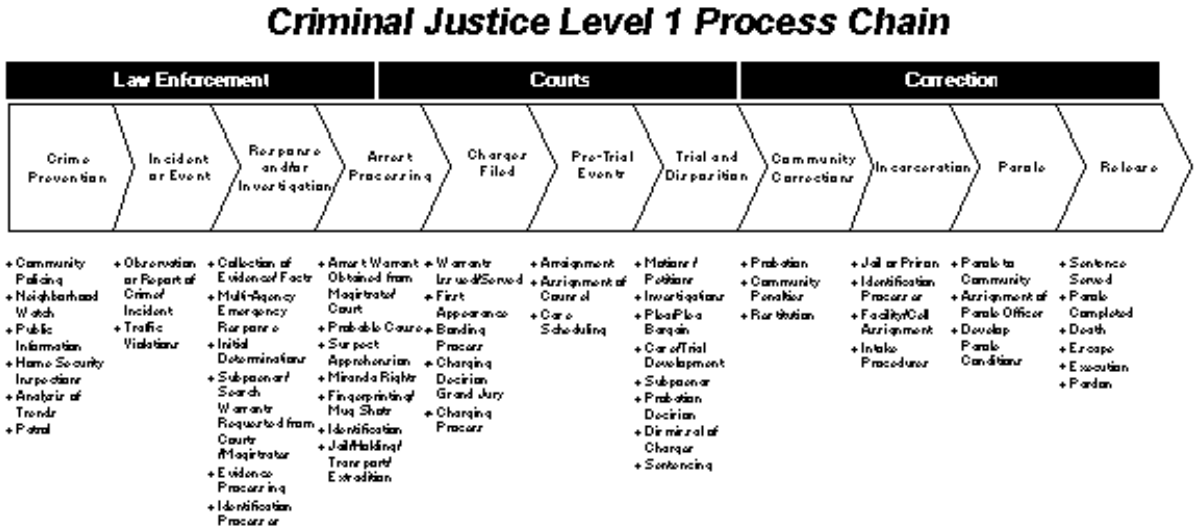

Criminal Justice Level 1 Process Chain
Law Enforcement
Courts
Correction
Crime Prevention
Incident or Event
Response and/or Investigation
Arrest Processing
Charges Filed
Pre-Trial Events
Trial and Disposition
Community Corrections
Incarceration
Parole
Release
+ Community Policing
+ Neighborhood Watch
+ Public Information
+ Home Security Inspections
+ Analysis of Trends
+ Patrol
+ Observation or Report of Crime/ Incident
+ Traffic Violations
+ Collection of Evidence/ Facts
+ Multi-Agency Emergency Response
+ Initial Determinations
+ Subpoena/ Search Warrants Requested from Courts/ Magistrates
+ Evidence Processing
+ Identification Procedures
+ Arrest Warrant Obtained from Magistrate/ Court
+ Probable Cause
+ Suspect Apprehension
+ Miranda Rights
+ Fingerprinting/ Mug Shots
+ Identification
+ Jail/Holding/ Transport/ Extradition
+ Warrants Issued/Served
+ First Appearance
+ Bonding Process
+ Charging Decision Grand Jury
+ Charging Process
+ Arraignment
+ Assignment of Counsel
+ Case Scheduling
+ Motions/ Petitions
+ Investigations
+ Plea/Plea Bargain
+ Case/Trial Development
+ Subpoenas
+ Probation Decision
+ Dismissal of Charges
+ Sentencing
+ Probation
+ Community Penalties
+ Restitution
+ Jail or Prison
+ Identification Procedures
+ Facility/Cell Assignment
+ Intake Procedures
+ Parole to Community
+ Assignment of Parole Officer
+ Develop Parole Conditions
+ Sentence Served
+ Parole Completed
+ Death
+ Escape
+ Execution
+ Pardon

Figure II-2

Missions and Critical Success Factors

An organization's mission statement is intended to describe the nature and concept of the organization's future business. It should establish what the organization plans to do and for whom, while substantiating the major philosophical premises under which it will operate. This statement forms the foundation for the rest of the strategic and operational plans and provides a common vision for the total organization. The primary reasons for an organization to have a mission statement are:

- To ensure a consistent, clear purpose throughout the organization;
- To provide a point of reference for all major planning decisions;
- To gain commitment from those within the organization by clearly communicating the nature and concept of the organization's primary business; and
- To gain understanding and support from people outside the organization who are important to its success.

While the design of a strategic plan around a core mission is quite common in the private sector, it is conspicuous by its absence in the government arena, and particularly rare within the justice community. This assessment is accurate for the criminal justice community in North Carolina at both the state and local levels. For many reasons, which are not within the scope of this study, the leaders in the criminal justice community either assume their organizations' future will be determined totally by legislative mandates or simply can be inferred by the history of their organizations' past activities. Regardless of the rationale, there is no consistent pattern of recently developed strategic plans built around the foundation of a clear mission. The mission statements which follow, therefore, are simply the most recent documents provided by the respective agencies and may not represent the full extent of what has been developed internally with regard to a strategic plan.

As a result of limited access to any strategic planning activities within the criminal justice community at the state level, some relevant information from the county level will be presented and reviewed as well. Together, these two sources of

information will, at least, serve to document the important level of congruence between the overall goals of the CJIN project and those of the individual state and local agencies.

Mission Statements for Key State Agencies

Mission statements were collected from the Judicial Branch of Government, the AOC, DOC, SBI, SHP, and the DMV and are recorded below.

The Judicial Branch of Government

The North Carolina Judicial Branch of Government defines its mission as follows: to protect and preserve the rights and liberties of all the people, as guaranteed by the Constitution and laws of the United States and North Carolina, by providing a fair, independent, and accessible forum for the just, timely, and economical resolution of their legal affairs.

Administrative Office of the Courts

The AOC is the organization that is responsible for administrative matters for the Judicial Department throughout the state. The mission of the AOC is to promote the highest quality justice throughout North Carolina's unified court system by providing administrative leadership, delivering efficient effective, and equitable administrative support and direct client services, and advancing sound business practices and solutions and system improvements.

Department of Correction

The mission of the DOC is to promote public safety by the administration of a fair and humane system which provides reasonable opportunity for adjudicated offenders to develop progressively responsible behavior. Further, it should be the duty of the department to provide the necessary custody, supervision, and treatment to control and rehabilitate criminal offenders and thereby reduce the rate and cost of crime.

State Bureau of Investigation

The mission of the SBI is to uphold the Constitution and enforce the laws of North Carolina by investigating crimes; analyzing evidence; identifying and apprehending criminals; and developing new investigative techniques and technologies, all in cooperation with fellow members of the greater law enforcement community.

State Highway Patrol

The mission of the North Carolina State Highway Patrol is to assure the safe, convenient, and efficient transportation of people and commodities upon the streets and highways; and, to reduce crime in our communities across North Carolina. This mission will be accomplished through reasonable and prudent law enforcement and quality service to the public based upon high ethical, professional, and legal standards.

Department of Transportation / Division of Motor Vehicles

No mission statement received.

Mission Statements for Key Local Agencies

The mission statements available at the local level included those for the Clerk, the Sheriff, the District Attorney, the Public Defender, and the District / Superior Court. Since these statements were collected from a single county, only broad generalizations can be made. The concepts presented, however, are basic enough to allow important comparisons with the mission of CJIN.

Clerk's Office

The mission of the Clerk's Office is to resolve disputes and assure compliance with legal mandates; to assure appropriate access to public records; and, to be the constitutional custodian of the state's court system records.

Sheriff's Department

The mission of the Sheriff's Department is to assure the safety and security of the public and those who work within the state court system through enforcement of both criminal and civil, state and federal laws.

District Attorney's Office

The mission of the District Attorney's Office is to assure just consequences for those who violate the criminal statutes of the state of North Carolina.

Public Defender's Office

The mission of the Public Defender's Office is to ensure to indigents accused of criminal offenses, and those civilly committed, the protection of all rights afforded by the constitutions of the state of North Carolina and the United States, and the laws of North Carolina.

The Courts (District and Superior)

The mission of the courts is to protect the rights of individuals and society, to promote peace and order by maintaining the rule of law, and to resolve disputes between and among persons, governments, and institutions through the interpretation and enforcement of the law.

Critical Success Factors of the Mission Statements

A review of the above statements reveals two key themes which need to be addressed. First, there is the public safety theme. Throughout the criminal justice system, there is the constant need to make decisions which safeguard the personal safety of law enforcement officers while they execute their primary duty of ensuring the safety of the citizens of the state. Second, there is the justice theme. While addressing the critical need for officer and public safety, the rights of individuals (particularly those of the criminally accused) must be protected as well. While the missions of some agencies

place greater emphasis on one or the other of these two themes, both themes must be incorporated into the mission of each organization and the conflicts between these themes must be recognized and resolved.

Critical Success Factors

A critical success factor is any factor which contributes significantly to the success of the organization's mission. A review of the above mission statements reveals at least five such factors which are relevant to the CJIN project.

First, there is the need for fairness. A person who is arrested should not be detained inappropriately or longer than necessary, should have access to timely legal counsel, and should be fully aware of the charges and the decisions made relevant to the disposition of the case. Any criminal justice information system designed must provide this information in the name of fairness. The fairness doctrine also applies to public safety. For example, victims and witnesses should be made aware of the status of a pending case, the disposition reached, and when the defendant is paroled, as these decisions affect their daily lives.

The second critical success factor relates to both the accuracy and completeness of the information. In support of public safety, the identity of the offender and his / her previous criminal history must be accurate. Law enforcement at the time of arrest, the magistrate at the time of bonding, the district attorneys at the time of trial, and the judge at the time of sentencing need this information to make quality administrative and legal decisions. For every citizen, there also needs to be protection against false arrest. It is not uncommon for a warrant to be served on the wrong person; a mistake which can have extreme consequences.

The third factor involves timely access to criminal justice information. Information which is accurate and complete, but not accessible in a timely fashion, is often irrelevant. Public safety, as well as officer safety, are severely compromised when an arresting officer has no information on outstanding warrants. Fingerprints, which may require two weeks to be processed, create a disadvantage for personal identification and subsequent prosecution. Similarly, when a person's probation or parole status cannot be accessed, there is the risk that this person will remain free and the violation unrecorded. And, finally, both at bonding and sentencing the judicial officers can only adjudicate with the information

available. Individuals who represent a danger to society may be released as the result of an inability to access important information in a timely manner. The rights of defendants are also at risk, if the public defender cannot determine the location of an incarcerated client, or a defendant can spend inappropriate time in jail waiting several weeks for a disposition to clear the system.

The fourth critical success factor apparent in the above missions is efficiency or the need to complete the most work, in the least amount of time using the minimum of resources. The entire criminal justice activity is a labor intensive operation with the bulk of each agencies' operating budget invested in people. Neither public safety nor justice is well served by an inefficient system where data is recreated and reentered a myriad of times for the same case across the various agencies. Not only is redundant data entry inefficient, but it also detracts staff attention and time from activities that would actually add value to the processing of criminal justice cases. This issue is also of great concern at the system level where repeated handling of data increases the risk of inaccuracy and the cost of its management. In addition, the lack of state standards locks counties into local systems and multiplies the costs of the development of incompatible systems statewide.

The fifth critical success factor related to these missions is effectiveness. While efficiency is focused on doing things right, effectiveness is directed at doing the right things. The difference between these concepts in outcomes is dramatic in that by focusing solely on efficiency, an organization runs the risk of doing the wrong thing well. Each of the missions state, or strongly infer, a quality component to their work. Any new information system design or enhancement cannot assume that the work practices engaged in currently are the best and need only to be automated. In fact, there probably is no worse decision in information system development than one which results simply in the automation of the current manual system. For this reason, both public safety and justice require that current work practices and existing statutes be reviewed to assure that they are still relevant and do not simply reflect the way things have always been done.

Implications for CJIN Study

The CJIN study was conducted with a clear understanding of, and respect for, the various missions of the law enforcement, courts, and correction communities. The projects recommended, along with the strategies designed for

their implementation, all reflect these individual missions and the collective need for a criminal information system which advocates both public safety and justice within each agency and across the state. To assure the maximum congruence between the missions of the agencies and the project recommendations for a new or enhanced system, special attention was given to incorporating one or more of the five critical success factors outlined above in each project.

Customers and Stakeholders

Stakeholders are the customers, individuals, and groups affected by, and capable of influencing, the change process. The identification of stakeholders and stakeholder issues is a valuable tool in determining the range of interests which need to be taken into consideration for planning change, and to develop the vision and change processes in a way that generates the greatest support.

Different stakeholders can perceive the same changes in quite different ways depending on their expectations of the proposed change; vested interests; existing pressures; affiliation; and priorities. With major change projects, the concerns, interests, and objectives of different stakeholders and stakeholder groups are frequently in conflict.

The main goals of a stakeholder analysis are to identify:

- who stands to gain or lose from proposed changes
- the primary forces for or against change
- factors influencing commitment to change
- key issues to be addressed during change planning
- possible avenues to better support change
- strategies for effectively managing change

To this end, a stakeholder identification session was conducted among the CJIN project team and project manager in order to fully share information gathered at the various focus groups, regional public hearings, and individual interviews conducted over the course of this project. A partial list of primary stakeholders, at various levels of state and local government, and within key agencies and organizations was developed by the project team and is presented below:

- Governor
- Chief Justice
- Attorney General
- General Assembly
- Constituents / Voters
- Secretary of State, as Chair of the IRMC
- Secretary of Correction
- Information Resource Management Commission
- Future's Commission of the Courts
- Parole Commission
- City or County Governments
- Judges
- Clerks of Superior Court (Clerk)
- Administrative Office of the Courts
- State Bureau of Investigation/ Division of Criminal Information
- State Controller
- CJIN Study Committee
- Department of Insurance
- Department of Correction/ Division of Adult Probation and Parole
- Department of Transportation/ Division of Motor Vehicles
- Department of Human Resources/ Division of Youth Services
- State Highway Patrol
- Sheriffs
- Police Chiefs
- Magistrates
- District Attorneys
- Public Defenders
- Juvenile Court Counselors
- Private Attorneys
- Victims / Witnesses / Defendants / Complainants
- General Public

Stakeholders can be further assessed across three primary themes and this information can then be used to determine funding resources, lobbying strategies, governance issues, and constraints.

Impact of Change

Proposed changes, identified as a part of the CJIN plan, will have a major impact on the various individuals and organizations involved in the criminal justice system. In assessing the potential degree of impact the proposed CJIN enterprise would have on key stakeholders, a label of "High" (H), "Medium" (M), or "Low" (L) can be assigned based on the overall impact of change across the following three broad categories:

- organizational structure
- culture and people
- business processes

Support for Change

The level of support and cooperation required from each stakeholder in order to achieve success can be assessed and classified as either "Necessary" (N), "Desirable" (D), or "Unnecessary" (U). Understandably, those stakeholders whose support is determined as "Necessary" are pivotal in the ultimate success of the CJIN initiative. Traditionally, in the government sector, stakeholders who are in key positions of power and / or control funding resources are labeled as "Necessary."

Factors Influencing Commitment to Change

A narrative assessment of those internal or external factors that influence a stakeholder's commitment to change can also be included. This helps in developing strategic approaches to the planning and implementation stages of a broad based change initiative, such as CJIN. Several broad categories should be considered when assessing a stakeholder's commitment to change including, but not limited to:

- Technical or functional advantages and disadvantages
- Control of resources
- Leadership

- Control of communications
- Hierarchical (organizational) advantages and disadvantages
- Legal or political implications

A synopsis of our stakeholder analysis findings is presented in the Stakeholder Analysis Matrix (Figure II-3) below. The summary information contained in this chart represents CJIN team members' opinions and observations and is not meant to be considered an exhaustive analysis of stakeholder issues, influence, or support. This information should not be regarded as comprehensive, but merely a "snapshot" of comments and impressions derived throughout the course of this project.

Figure II - 3 Stakeholder Analysis Matrix

Stakeholder	Importance of Support	Impact	Factors Influencing Change
Governor	N	L	Voter support required
General Assembly	N	L	Funding authority
Constituents / Voters	D	M	Citizen reaction to system weaknesses/ failures drives change
Secretary of State	N	L	Supports CJIN initiative
Chief Justice	N	H	Primary focus on courts and AOC
Administrative Office of the Courts	N	H	Funding issues; separation of powers - judicial branch
Attorney General	D	L / M	Primary law enforcement focus

Stakeholder	Importance of Support	Impact	Factors Influencing Change
State Bureau of Investigation	N	H	DCI is one of the primary agencies in the new CJIN
Secretary of Correction	N	L / M	Supports integration of criminal justice information with DOC
Department of Correction	N	H	CJIN complements new OPUS system
Division of Probation & Parole	D	H	OPUS system will help reduce current redundant data collection and entry
Department of Insurance	D	M	Focus on tracking bond information
Department of Transportation/ Division of Motor Vehicles	D	M	Information needs from law enforcement are high
State Highway Patrol	D	H	Primary focus on 800 MHZ system and criminal history access
Sheriffs	N	H	Officer safety issues paramount; local political strength in some areas
Police Chiefs	N	H	800 MHZ priority; local user fees issues
Information Resource Management Commission	N	M / H	Governance of CJIN at issue with current role of IRMC
Future of the Courts Commission	D	M	Primary focus on court reengineering

Stakeholder	Importance of Support	Impact	Factors Influencing Change
City or County Governments	N	H	Support varies based on vested interest/local politics / local systems or lack thereof
Judges	D	M / H	Workload efficiency and decision making benefits
Clerks of the Superior Courts	N	H	Overall substantial operational changes; personnel functional considerations
Magistrates	D	H	Cost savings and efficiency improvements prove to be substantial with automated magistrate system
District Attorneys	N	H	Desirous of accurate timely CCH information
Public Defenders	U	H	Currently request CCH information from DA's - time delays would be reduced
Private Attorneys	U	H	Would like access to clerk information remotely via PC / modem
Victims / Witnesses / Defendants / Complainants	U	H	Portion of public in direct contact with justice system

Change Driver Analysis

Change drivers are those critical events or forces that affect an organization's ability to do business. By identifying and maintaining focus on key change drivers, the CJIN project can maximize the many internal and external influences and ensure a successful solution. The following is a brief summary of the change drivers that have been identified through focus groups, interviews, and public hearings.

The Reduction, and Ultimate Elimination of Inefficiency and Redundancies

- North Carolina's increasing population, and the increasing attention on reducing crime, strains the criminal justice system at all levels by increasing the cost of policing, administering justice, and incarcerating offenders.
- The lack of common statewide offense codes results in multiple agencies recoding information to fit their own standards.
- The lack of integrated automation often results in the rekeying of already automated information at agency hand-off points.

Public Demand For Increased Safety

- The public's fear of increasing crime and personal safety has driven citizens to demand greater accountability from all criminal justice agencies including local and state law enforcement, the courts, and correctional agencies. This demand translates into a need for more timely and accurate information to and from all agencies within the criminal justice arena and the need for more effective management of resources.
- New victims' rights legislation mandates the provision of information to communities on the release of offenders, conditions of parole and probation, and court appearances among others.

- The publics' increasing frustration with the release of individuals, at various points in the criminal justice system, whom they perceive as dangerous and / or detrimental to society has put substantial strains on the system as a whole.

- Increased political support for improved criminal justice systems has been in part due to constituent pressures and demands. The Governor's Crime Commission was established specifically to address the public's dissatisfaction with crime and to develop target approaches to improving the criminal justice system as a whole.

- An inability, at the magistrate level, to properly identify individuals and to access criminal history in order to properly charge and determine bond requirements is a potential detriment to public safety.

Agencies' Demands for Accurate, Compatible, and Timely Information and Cross-Agency Communications in Order to Fulfill Missions, Goals, and Objectives

- The USAir plane crash near the Raleigh-Durham Airport during the fall of 1994, poignantly demonstrated various emergency response agencies' inability to communicate with one another, greatly hampering coordinated response activities and reflecting negatively on various agencies' efforts.

- Up-to-date disposition and offender release information is necessary in order for law enforcement to effectively police communities.

- Lack of a common statewide automated identifier, such as AFIS, results in higher rates of misidentification and excessive time and effort involved in the identification process.

- Structured sentencing legislation has pushed the courts to demand timely and accurate criminal history information in making appropriate sentencing decisions.

Aging Technology and the Need for Immediate Improvements and Additions to the Technical Infrastructure

- Aging and proprietary technology currently in place at various criminal justice agencies does not easily meet the need to share necessary information in an automated fashion.
- Various criminal justice agencies independently submit budget requests for technology improvements, without integrated planning for system compatibilities and shared access.
- Individuals, from all walks of the criminal justice system, are becoming more familiar with available technologies and desire better ways of doing business.

Overall Criminal Justice System Fragmentation

- The organization of judicial districts and law enforcement jurisdictions causes fragmentation and a possible duplication of efforts, as well as a possible under-utilization of existing resources.
- The combined information needs of the juvenile justice system, the welfare system, and the adult criminal justice system are not currently being met.
- Highly centralized state systems need to be flexible enough to accommodate the different needs of communities and local criminal justice providers across the state.
- Lack of integrated mobile voice and data systems hamper local and state law enforcement communications and suspect identification processes.

Current Information Systems Environment

The existing criminal justice information systems' environment is comprised of hardware and software systems from multiple agencies. This section presents an overview of the existing North Carolina state-level criminal justice applications, databases, hardware, and networks. Only the state components with relevance to the entire justice enterprise are covered within the subsections. For example, the State Bureau of Investigation's overtime tracking system is intentionally omitted from the application subsection.

This section provides an understanding of the basis from which to build CJIN. An understanding of this basis is crucial to identify areas of strength and weakness and make migration recommendations. There are four areas covered within this section:

- Applications and Interfaces
- Databases
- Hardware
- Existing Criminal Justice Network

Applications and Interfaces

This section lists both applications and interfaces for the Administrative Office of the Courts, Department of Correction, State Bureau of Investigation's Division of Criminal Information, and Division of Motor Vehicles. Only the applications and interfaces with relevance to the entire network are listed. Identification of these programs assists in recognizing current system strengths, reengineering opportunities, and new system requirements.

AOC Criminal Applications and Interfaces

Applications	Interfaces
• Court Information Systems Criminal Infractions • District Case Management • Financial Management System General Ledger Accounts Payable Jury Payment Partial Pay Distribution • Mainframe Cash Receipting→PC Cash Receipting • Child Support • Set-off Debt • Statistical Reporting System • Civil Indexing • State Highway Patrol Computer Aided Dispatch	• AOC Local Interface (ALI) • Division of Criminal Information • Department of Correction • State Highway Patrol • Division of Motor Vehicles

DOC Applications and Interfaces

Applications	Interfaces
• Inmate Population Tracking • Offender Reception Process • Offender Time Computation • Probation and Parole Supervision • Inmate Activities • Inmate Control Status • Inmate Custody Classification • Inmate Monitoring & Transfer • Mental Health Services • Medical Services • Investigative Tracking • Court Ordered Payments • Work Release System • Safekeeper Billing	• Administrative Office of the Courts • Division of Criminal Information

SBI / DCI Applications and Interfaces

Applications	Interfaces
NCIC / DCI "Hot File" Applications • Wanted Persons • State Wanted Persons • Missing Persons • Unidentified Persons • Stolen Vehicles • Stolen License Plates • Stolen Boats • Recovered Vehicles (State Only) • Stolen / Recovered Guns • Stolen Articles • Stolen Securities	• Department of Correction • Administrative Office of the Courts • Local CJIS • State Bureau of Investigation
FBI / DCI Criminal History Applications • Interstate Identification Index (III) • Computerized Criminal Histories (CCH)	

NLETS Capabilities • Interstate and Interagency E-mail • States' DMV access • National Insurance Crime Bureau access (NICB) • Canadian Police Information Center access (CPIC) • Online inquiry to state and local criminal history record information • Online transactions to the Aircraft Tracking and Registration System	
DCI Mapper Applications • Summary UCR and IBR systems • SBI Case Records • SBI Laboratory System • SBI Criminal Intelligence System • SBI Major Special Investigations • State Homicide and Assault Reporting System (SHARE) • Drug Data Entry System • Vehicle Identification Number (VIN) Check Calculation	

DMV Applications

Applications	Interfaces
• State Automated Driver License System (SADLS) • Commercial Drivers' Licensing System access (CDLIS) • Drivers' License Registry access (DLR) • Problem Driver Pointer System (by 4/95)	• AOC Interface • DCI Interface

Databases

State agencies currently use a number of different database management systems (DBMSs) to store and retrieve data. Providing communication between these diverse platforms poses a significant challenge to building a CJIN. The following table displays the DBMSs each agency employs.

	AOC	DMV	DOC	SBI
ISAM				✓
VSAM	✓	✓	✓	
IMS	✓			
DB2	✓	✓	✓	
DB2 / DB400		✓		
Unisys DMF				✓
Unisys RDMF				✓
Unisys Mapper				✓
Sybase		✓		

Hardware

The existing state-level criminal justice systems consist of hardware systems from multiple agencies including:

- State Bureau of Investigation, Division of Criminal Information systems
- Administrative Office of the Court system
- Department of Correction State Information Processing Services (SIPS) data processing system
- Department of Transportation, Division of Motor Vehicles SIPS data processing system

The following table provides a summary of the existing North Carolina criminal justice computer infrastructure used by the member agencies and organizations.

System	SBI / DCI	AOC	DOC / DMV
Mainframe system	Unisys	IBM	IBM
Minicomputer system	N / A	AS/400	N / A
Server system	Printrak AFIS, Unix	NetWare, Unix	N / A
Protocols supported	Uniscope, TCP/IP, SDLC, BISYNC	SDLC, TCP/IP	SDLC, TCP/IP
Workstation type	Uniscope	3270	3270
Personal computer	PC	PC	PC

Existing Criminal Justice Network

The existing state-level criminal justice network is a wide-area network of interconnected agency and state computer systems. The SBI and AOC agency computers and networks, together with SIPS data processing centers supporting the DOC and the DMV, are currently interconnected by application specific communications links.

Current AOC Network

The current AOC network consists of local and wide-area links to the AOC mainframe computer. AOC terminals and PC workstations are connected to the mainframe via IBM SDLC communications links. The enclosed diagram provides a high-level view of the existing AOC network.

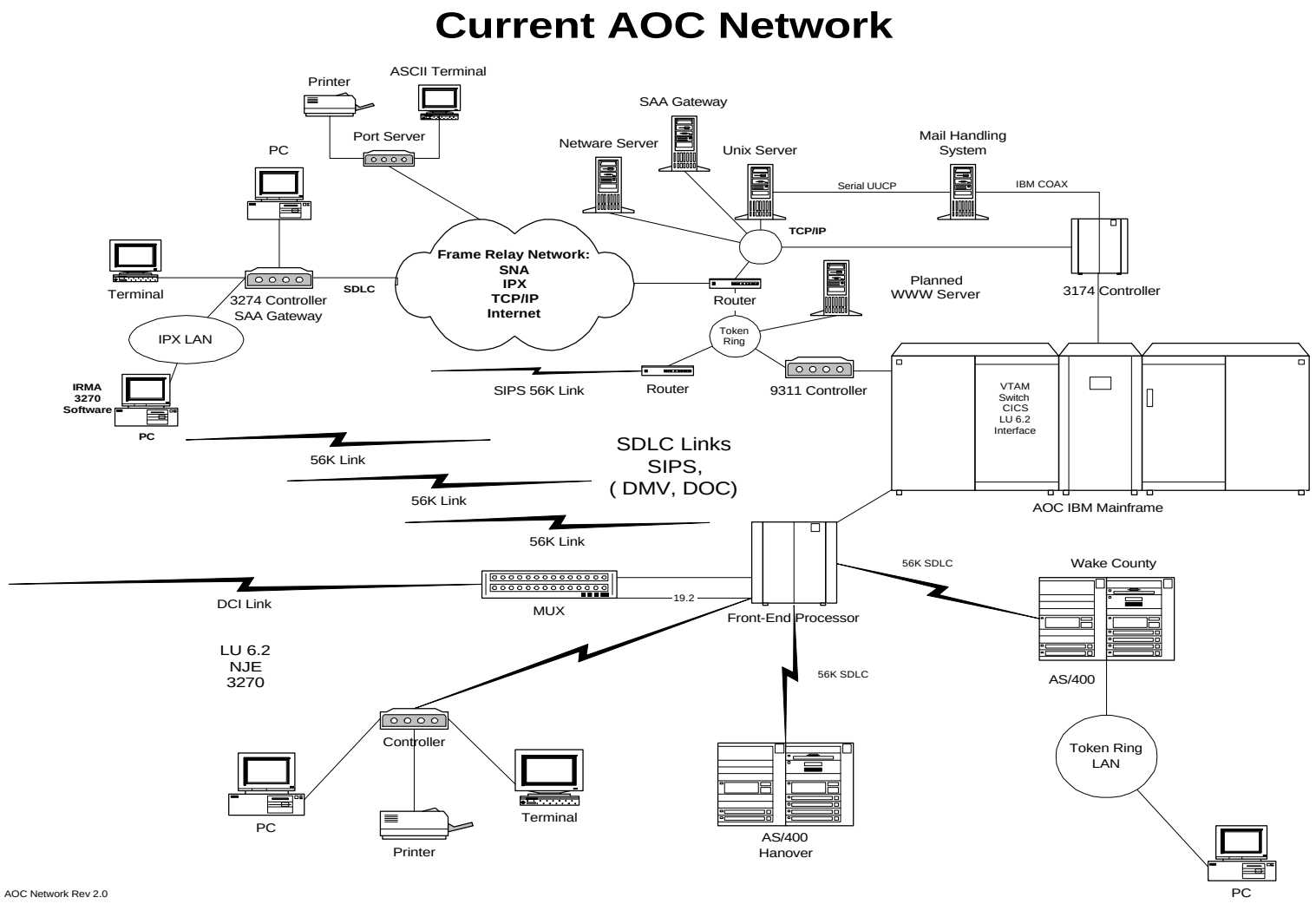

Current AOC Network
Printer
ASCII Terminal
Port Server
PC
SAA Gateway
Netware Server
Unix Server
Mail Handling System
Serial UUCP
IBM COAX
TCP/IP
Terminal
3274 Controller
SAA Gateway
SDLC
Frame Relay Network:
SNA
IPX
TCP/IP
Internet
Router
Planned
WWW Server
3174 Controller
IPX LAN
Token Ring
IRMA
3270
Software
PC
SIPS 56K Link
Router
9311 Controller
VTAM
Switch
CICS
LU 6.2
Interface
56K Link
SDLC Links
SIPS,
(DMV, DOC)
56K Link
AOC IBM Mainframe
56K Link
56K SDLC
Wake County
DCI Link
MUX
19.2
Front-End Processor
LU 6.2
NJE
3270
56K SDLC
AS/400
Controller
Token Ring
LAN
PC
Terminal
AS/400
Hanover
Printer
PC
AOC Network Rev 2.0

Figure III-1

Current SBI Network

The current SBI network consists of local and wide-area links to the SBI computer center. SBI and DCI terminals and PC workstations are connected to the UNISYS mainframe using a variety of communications links employing Unisys Uniscope, TCP/IP, BISYNC, and SDLC protocols. The enclosed diagram provides a high-level view of the existing SBI network.

Current SBI Network

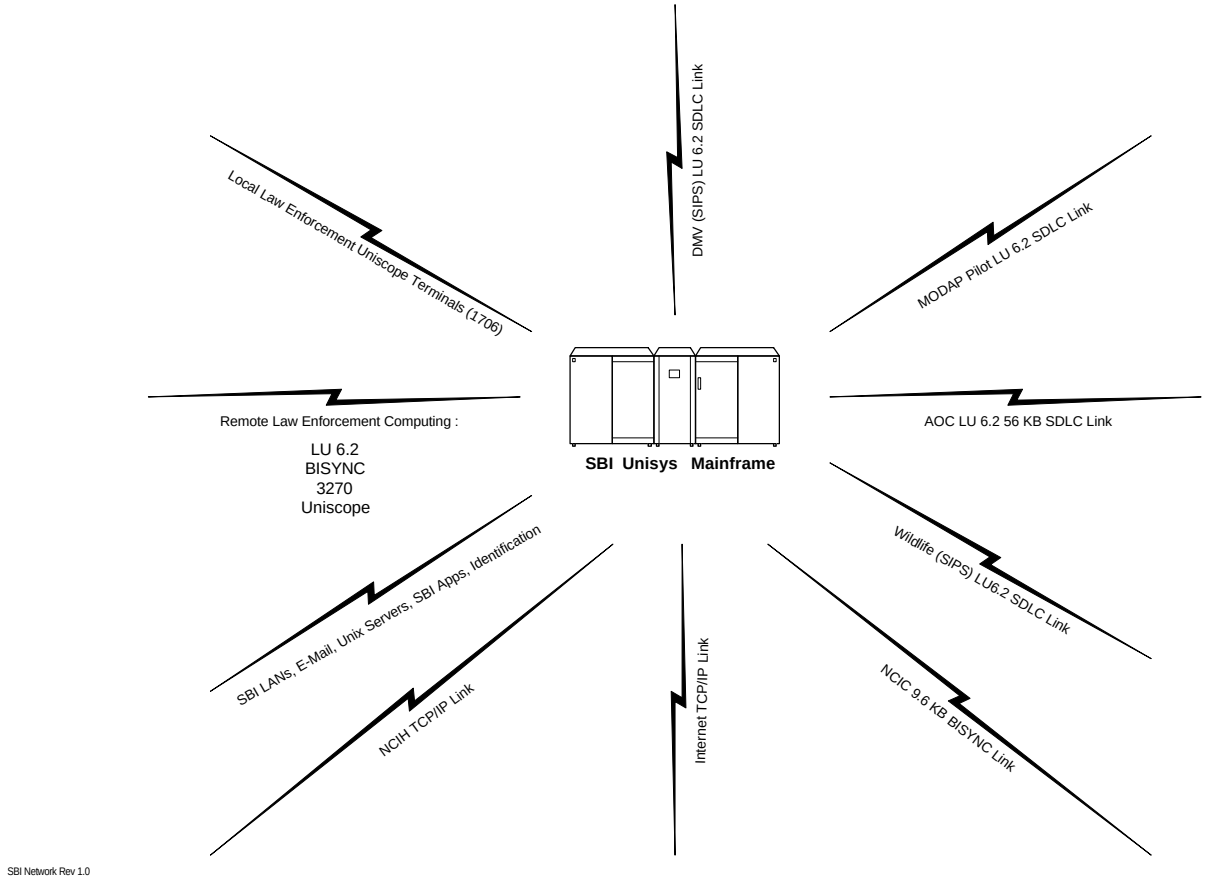


Figure III-2

Current SIPS Network

The current SIPS network consists of a state-wide digital communications network. SIPS provides data processing services for the DOC and the DMV. SIPS computers are connected to the AOC computer system and the NCIH. DOC and DMV terminals and PC workstations are connected to SIPS data processing systems via IBM SDLC communications links. The enclosed diagram provides a high-level view of the SIPS mainframe system for the DOC and the DMV and the associated link to the AOC computer system.

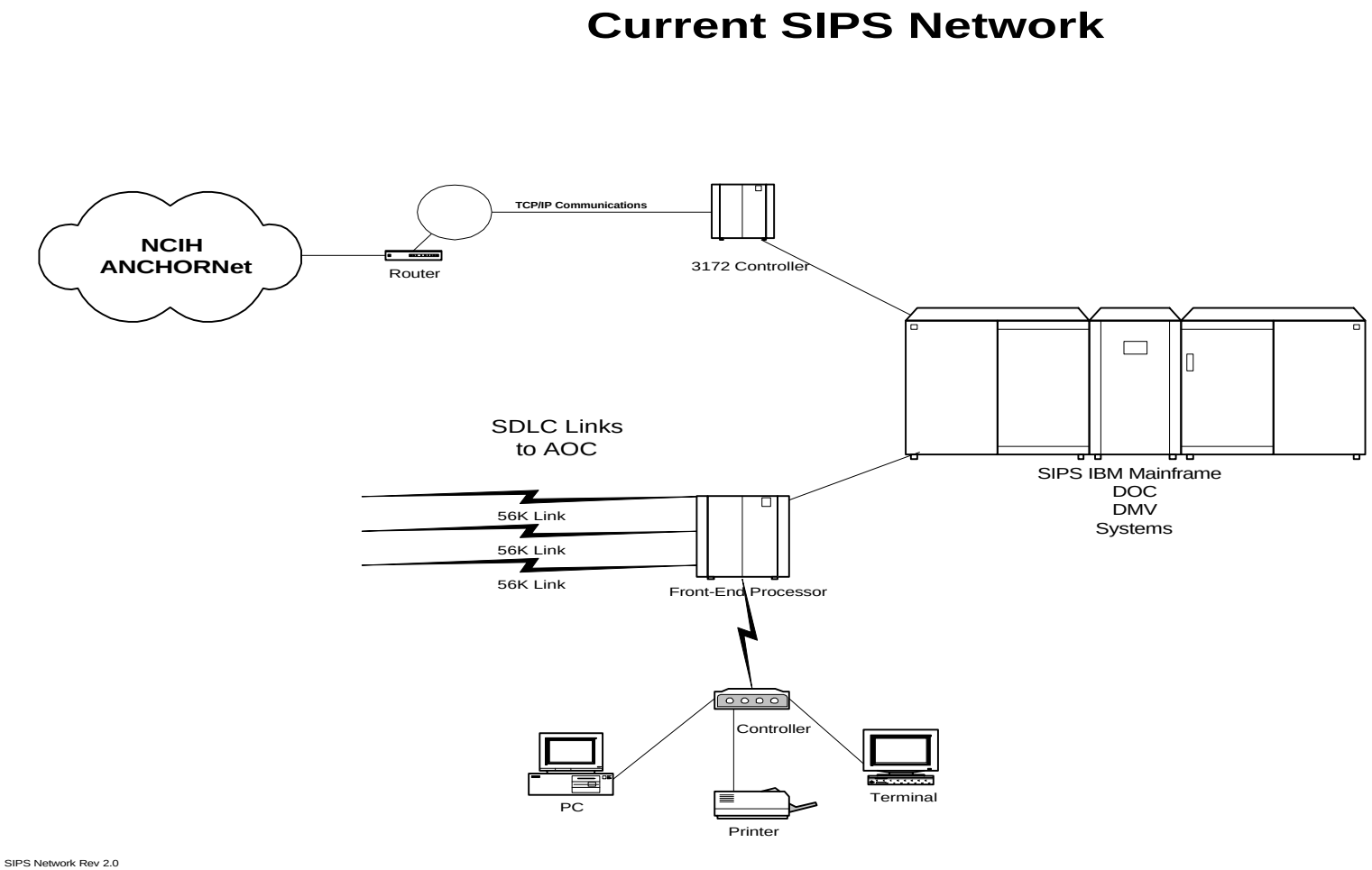

Current SIPS Network
NCIH
ANCHORNet
Router
TCP/IP Communications
3172 Controller
SDLC Links
to AOC
56K Link
56K Link
56K Link
Front-End Processor
SIPS IBM Mainframe
DOC
DMV
Systems
Controller
PC
Terminal
Printer
SIPS Network Rev 2.0

Figure III-3

CJIN Governance Strategy

The recommendations in this study necessarily need to be complemented by options for how the proposed CJIN enterprise will be structured and governed to assure effective administration. While progress has been made on interagency sharing of information on an informal basis, full realization of the benefits from the investment in isolated systems requires an enterprise wide governance structure. To a large extent, the credibility of the technical recommendations will be determined by the leadership strategies proposed to guide their implementation. In the discussion of the leadership models that follows, the scope of CJIN governance, and the functions to be performed by the governing body, are indicated first in order to provide a rationale for the subsequent structure and membership recommendations. The logic employed in presenting the information in this sequence is based on the need to decide first what needs to be done by a central group (board) and only then to determine the nature of the group that could best perform these functions.

Scope of Governance

The goal of the governance models is to design a broad management structure that assures compatibility and accessibility of all information relevant to the criminal justice system as created or utilized by criminal justice agencies at both the state and local levels. We do not envision a controlling agency with invasive micro management of state or local agencies. In fact, nothing in this plan is intended to infringe on either the separation of powers or the operational integrity of any agency. The clear intent is for the core functions of existing agencies (e.g., AOC, SBI/DCI) to remain with those agencies, but with enhanced abilities to integrate these functions across affected agencies.

While focus on the criminal justice portion of the overall justice system is broad, it does not address directly three other important sets of relationships that deserve recognition and subsequent attention. First, there are agencies, such as the Department of Transportation (DOT), that may not be included under a CJIN governance structure, but whose data standards and operations directly affect the criminal justice system and vice versa (e.g., DMV in areas of vehicle registration, DUI, and citations). Interdependence with such agencies needs to be recognized and managed by direct

coordination between the Information Resource Management Commission (IRMC) and the managing body for CJIN.

Second, the Administrative Office of the Courts (AOC) manages information relevant to both the criminal and civil components of the justice system. While the civil portion, by definition, will not fall under CJIN governance, many of the criminal justice related projects will be relevant for the civil side and should be leveraged to enhance civil case processing to the extent possible. We recommend that this issue be referred to the Commission for the Future of Justice and the Courts in North Carolina, which has a mission that encompasses both the criminal and civil domains.

Third, consideration needs to be given to the entire juvenile area. The delinquency portion falls under CJIN governance while the dependency side will continue to be under the authority of the Department of Human Resources. Similar to the situation with the DOT, it is important that technology and data standards issues be coordinated between the juvenile delinquency and dependency areas by strict adherence to IRMC standards, and managed by direct coordination between the IRMC and the managing body for CJIN.

In each of the above three situations, it is important to recognize that coordination efforts outside the recommended formal governance structure are essential and will benefit each agency and the overall enterprise as well. While the dichotomization of criminal and civil, and delinquency and dependency may be necessary to stay within the criminal justice scope of this study, real world situations demand coordination and the maximum leveraging of technology between related areas as well. In the end, no governance system can or should be structured to manage all contingencies. At some point, common sense and a commitment to serving the public need to prevail.

We recommend that the appropriate administrative model for the mobile voice and data system be addressed separately. The rationale for this approach and recommendations concerning this issue are presented in Section VI.5 - Statewide Mobile Voice and Data project.

In light of the above issues and exceptions, the following governance issues are presented. The discussion presents the critical functions to be performed, within the above scope, by the governance structure; the principles that should guide its governance activities; three possible models by which this could be accomplished; our recommendation; and the criteria that should be used to measure the effectiveness of the recommended governance model.

Critical Functions

The primary functions that the governance group will need to perform are:

1. **Develop and maintain technical standards** - An integrated network with functional integrity needs standards in at least the following three areas:

   - Unique CJIN data standards and communications protocols, which extend beyond those established by the IRMC, such as the application areas of fingerprints and criminal history.

   - Business definitions of key data elements and the business rules required to guide these definitions (e.g., the offender's name will be recorded in a standard fashion, charge codes will be used which include a specific number of digits and format).

   - Standards for changing business definitions and the related rules and methods for coordinating changes between organizations - change should be compatible both forward and backward in time, as well as upward and downward in the organization. The implications for both state and local systems must be taken into consideration.

   (NOTE: In order for a governance group to perform the above functions, it will be necessary for the General Assembly to adopt statewide standards or empower the standard setting body, and to require city or county agencies who request state funds for technology to abide by these standards. This mandate would not preclude local governments from developing and funding their own local systems as long as these systems were compatible with the state standards and did not jeopardize the ability of other local or state agencies to access data statewide.)

2. **Evaluate present technology in relationship to future options and applications** - This function addresses strategic planning designed to envision the future needs of the system, and to determine the changes required to position the information system to respond to priority needs. The group will be charged to perform a

"proactive" leadership role whereby it will monitor broad based changes in technology pertinent to the state system and make recommendations for changes or enhancements in a deliberate, thoughtful, and non-reactive manner. This function will include:

- The identification of technological opportunities, cost-benefits, and positive yield statewide.

- Research and development involving new technologies relevant to the criminal justice system along with the reengineering of existing processes required to gain maximum synergy. Without such reengineering the benefits of technology will likely be constrained by inefficient or incompatible processes and procedures.

- The monitoring and dissemination of best practices from within the state and across the country which have statewide application. Some local jurisdictions already have advanced systems that are scalable and portable to other counties or even statewide. Other states, in turn, will continue to evolve and their efforts need to be monitored for possible application within North Carolina.

3. Administration - This function involves the business administration of the CJIN enterprise and includes:

- An advocacy role with the General Assembly to advance CJIN projects which affect multiple agencies and foster the development of a statewide criminal justice information network.

- Coordinate, specify, and "champion" bids through normal state contracting processes for specialized equipment and services to gain the best contracts for all users and assure financial accountability where state funds are used.

- A liaison role with state, county, and city officials to guide their financial and systems planning for automation. Communications regarding statewide directions will be important to these decision makers to ensure compatibility of equipment and systems and to coordinate the timing of such purchases. The role of CJIN governance would be to articulate these directions in a timely manner.

- A fundraising role which would include the design of innovative approaches for funding the system on a continual basis from resources internal to the state, and for securing funding from federal agencies and foundations in support of the system.

- A financial management role in administration of appropriated funds and funds procured from other non-appropriated sources. These funds would be used for:
  - the needs of small, local government entities
  - the development and exporting of elements of the system that lie within the local governments responsibility
  - the development of elements of the system which are state responsibilities when the development is a joint venture between state and one or more local governments
  - interface projects between state agencies.

These funds would not be intended to supplant appropriations to state agencies to make large scale system improvements in an agency's sphere of operations.

Principles of CJIN Governance

In each of the regional public hearings, the focus groups, and throughout the personal interviews, the topic of governance for CJIN was addressed. And, while there was no one clear and common model suggested, there was a definite consensus on the principles upon which any governance system should be based. These principles are described briefly below and are followed by three specific forms of governance structures which incorporate these principles. The key principles are:

1. **Political independence** - This factor is not intended to provide a governance structure free of political oversight or accountability, but rather to create one that transcends the politics of any one state agency, while acknowledging and respecting the separation of powers that exists between the three branches of government. The issues of crime, public safety, and government efficiency are not limited to any one agency nor can they be fully addressed by the efforts of any single entity. In essence, the governance structure of CJIN should reflect the

systemic nature of the problems that exist and the level of interagency cooperation which will be required to address them.

2. **User representation** - There is an ongoing and dynamic tension in the governance process created by the challenge of trying to balance the needs of the state for administrative coherence with the needs of local government for flexibility. It is particularly critical in the area of criminal justice as much of the work is done at the local level. The governance structure designed for the CJIN enterprise should therefore include, at a minimum, state and local representation from the three areas of law enforcement, the courts, and corrections. In addition, special coordination efforts will be required with such agencies as DOT's DMV and DHR's Department of Youth Services even though not under the direct CJIN governance. The philosophy which undergirds this principle is the belief that the higher in the organization a problem is recognized as being important, the more likely it is to be addressed, and the lower in the organization the solution is identified, the more likely it is to work. Extensive efforts have been made to assure the users that the goal of CJIN is not to develop a centralized state system, but rather a system that meets the needs of users statewide. The credibility of CJIN governance will be proportionate to the degree to which users are represented and influential at the policy level on an ongoing basis.

3. **Service orientation** - One concern voiced throughout the study was the fear that CJIN will result in one more bureaucracy whose mission is to control and audit local jurisdictions and, consequently, create barriers to local jurisdictions' ability to solve their problems in an effective and expedient manner. The alternative and preferred model would be one of an agency committed to service, and to equipping and facilitating local jurisdictions to be successful in meeting their local needs based on a model of statewide integration. Once minimum statewide standards are developed and accepted legislatively, CJIN's role, as outlined above, should be primarily one of assisting local users in gaining maximum connectivity to the databases appropriate for their work and of brokering ideas that provide long-term system stability. In this regard, the size of the CJIN board should be relatively small as should be the CJIN staff (i.e., four to five technical experts in addition to an Executive Director and secretary) as further confirmation of their critical, but limited role.

4. **Board representation and selection** - The CJIN board members should be appointed by their respective political authority (see models below) and be individuals who are both knowledgeable about the issues facing the criminal justice system and committed to addressing them. A full time Executive Director, who has a vision for the needs of the state and knowledge of the technology required to achieve that vision, should be hired by and report to the board. This person should have sound organizational and financial management skills and experience. A national search should be conducted by the CJIN board to recruit the best talent available and the board should be prepared to provide a salary and benefit package that reflects the importance of the position. The CJIN staff should be comprised of four to five technical experts in the areas of law enforcement, courts, corrections, and telecommunications who would, along with the Executive Director, form a high performance team of consultants and research and development resources. These individuals should be full time, recruited nationally, and compensated appropriately for their skills and contribution to this statewide enterprise. The funds for the Executive Director and staff should be allocated to an existing state agency such as the Office of State Budget and Management for purposes of disbursement and accounting. We recommend that positions and numbers be reviewed after one year.

Structures for CJIN Governance

The prompt and thoughtful resolution of the governance structure issue for the CJIN enterprise is one of the critical success factors for the entire project. The successful creation and funding of this group will not only provide the identity and focus required to communicate the statewide nature of the overall project, but it also will provide the leadership and continuity required to assure the long-term viability of the criminal justice information network independent of political transitions in state and local leadership.

The purpose and principles discussed above are used as the foundation for the development of the following three governance options. For each model, specific advantages and disadvantages are included. It should be noted that other options were discussed in the course of the study, which are not included as models such as the addition of AOC representation to the current IRMC; the reorganization of the IRMC to create balanced representation from all branches of government; and the expansion of the role of either the AOC, Department of Justice (DOJ), Office of State Controller

(OSC), or State Information Processing Services (SIPS) to include the full spectrum of criminal justice operations. These options were not considered viable for CJIN and are not further discussed.

Three possible options for the governance of the CJIN enterprise are:

1. **A separate CJIN board within the current IRMC** - One option is to create, and establish through legislation, a standing CJIN subcommittee within the IRMC. The CJIN board would consist of approximately ten members appointed respectively by the Governor (2), the Attorney General (2), the Chief Justice (4), the President Pro-Tempore of the Senate (1), and the Speaker of the House (1). One or two of these members should be from the private sector and academic community with at least one half of the board members being selected from local jurisdictions. The Executive Director of CJIN would be hired by and report directly to this board, which would be chaired by a member-at-large.

   The advantages of this model (which has a precedence in the Geographic Information System's (GIS) reporting relationship with the IRMC) are:

   - Specific identity and recognition of CJIN as an entity focused on the criminal justice system statewide.
   - Clear and singular lines of authority for the Executive Director and the staff.
   - Direct involvement of users at the policy level.
   - The ability to coordinate CJIN policies with those of the IRMC (i.e., the requirement to meet IRMC standards except where variance is granted by the larger IRMC board).

   The disadvantages of this model are:

   - The inclusion of judicial branch representation in a group currently established by statute to oversee only executive branch agencies.

- The recruitment of additional staff.
- Potential conflict in staffing responsibilities (i.e., the Office of the State Controller's Information Resource Management (IRM) Division provides staff support to the IRMC, but does not provide technical support for the AOC).
- The creation of internal competition for resources between the executive and judicial branches.
- Potential conflicts in the concurrent development of statewide standards (although CJIN would only add standards to what the IRMC has established).
- A break in continuity as political leadership changes.
- Increased management efforts that would be required to assure coordination between the CJIN and the IRMC board policies and directions. This issue could be addressed partially by having the chairperson of the CJIN board sit as a full member on the IRMC board.

The primary intentions in this first option are to build on a known entity (i.e., the IRMC) and on the precedent of an independent subcommittee within this existing agency (i.e., GIS). In a review of this model with the various constituent groups, there was a strong concern raised as to whether this model would truly provide the independence warranted for the judicial branch without a major restructuring of the statutory mission of the IRMC.

2. **An independent board within state government** - A second option is to create the same CJIN board as described above, but with an organizational status outside of the IRMC. A major issue cited is conformance to, and coordination with IRMC standards to achieve statewide interoperability. This could be accomplished through precise legislation that requires CJIN technology meet IRMC standards to qualify for state funding, and through reciprocal representation between the two groups (e.g., the IRMC chair could be an automatic member of the CJIN board and the CJIN chair could sit with full membership as part of the IRMC board). The CJIN

board itself would not have to be a subcommittee of the IRMC to accomplish these primary results. There would, however, need to be a commitment from the leadership of CJIN to consult and communicate regularly with the IRMC to maintain the highest level of compatibility of information system developments statewide. And conversely, there must be a commitment from the IRMC to promptly facilitate the resolution of CJIN related issues and to respect the defined mission of CJIN.

In addition to the advantages cited for the first model above, this model would:

- Guarantee the clear separation of powers for each branch of government.
- Provide a clear identity for the CJIN enterprise with a focus on the criminal justice information system statewide.
- Provide a more direct and singular reporting relationship for the Executive Director and CJIN staff.
- Simplify and clarify approval procedures for technology development (i.e., current executive branch agencies such as SBI / DCI and DOC would only process requests through CJIN for those projects which affect the criminal justice system statewide; otherwise, they would report directly and only to the IRMC, while the AOC would report directly and only to CJIN for approval regarding standards).
- Clarify quality assurance standards and procedures (i.e., the oversight for the AOC would be provided within the judicial branch and the oversight for executive branch agencies would continue to be provided by the IRMC).
- Establish a specific policy development role that transcends the three branches of government.

The disadvantages of this model are:

- The creation of a new organization (board) and the precedent this would set within the state. This should not prove to be a major disadvantage, however, since the rationale for a separate CJIN board is warranted by the need for the separation of powers, which would not be true for executive branch agencies currently reporting through the IRMC.

- The potential of a dual reporting relationship for executive branch agencies when their projects affect the criminal justice activities.

- The need for tight coordination regarding standards (e.g., if a DMV proposal to the IRMC affects a clerk's office or an AOC proposal affects the DMV, these issues would need to be resolved through collaboration between the IRMC and CJIN).

3. **A private management group model** - With regard to the issue of independence, a third model and its rationale are presented as well. While the first two options represent configurations within state government, another option is to privatize the CJIN governance structure and out source it to a vendor knowledgeable in the criminal justice field.

   The advantages of this model would be:

   - Perceived and actual independence (i.e., it would be apolitical, not just politically balanced).

   - A high level of technical and business management expertise.

   - Easy access to current and future technologies, technical training, and assistance.

   - A contractual relationship that would keep the focus squarely on performance for continuation of the contract.

   The disadvantages would be:

- A lack of connection to the political structure of the state with possible increased difficulties in competing for state funds.

- A concern, at least on the part of the General Assembly, about accountability.

- Greater difficulty in coordination with the IRMC.

- Concerns regularly associated with managing a public - private relationship.

More important than the suggestion of this model, however, are the concerns that motivated it. Throughout the study, constituents indicated they were apprehensive about the ability of state government to create a governance model that is independent enough to address the issues in a timely fashion, make decisions that are truly best for the criminal justice information system statewide, and foster the entrepreneurial mindset necessary to realize the vision of the CJIN enterprise.

While interagency cooperation is well regarded in the present political culture, the vision for the CJIN enterprise is without a clear operational precedent. Not only will all branches of government need to cooperate along with their respective agencies, but there also will need to be vertical integration between the state, all counties, and local communities as well. The strategic decisions that the CJIN board will need to make should not be held hostage by lengthy political negotiations or turf battles, or diluted by compromises that reflect only political expediency at the expense of system effectiveness. A private business model was thought by some to best address or even avoid these concerns.

Recommendations

We recommend adopting the second model - an independent board within state government. This option, when created by statute, will provide the necessary independence required for effective functioning by the CJIN board and its Executive Director, and staff, while still ensuring the important and appropriate level of coordination and consultation

with the IRMC with respect to standards. In addition, it will transcend, yet pull together, all three branches of government and provide for user involvement at the policy level with a clear and visible identity for the criminal justice system statewide. And finally, this model will allow the CJIN board to focus its efforts on statewide issues while best representing the needs of local users.

Measures of Effectiveness

There are several key issues the CJIN governance group will need to address initially and throughout its work which will determine its ultimate effectiveness. These issues are:

1. The establishment of the standards necessary to achieve the connectivity required between counties, counties and state agencies, and the state agencies themselves. This effort should build on the recommendations of the CJIN study, but limit the number and specificity of the standards to only what is absolutely necessary to achieve an ongoing level of systemwide integration.

2. The establishment of policy authority to enforce the standards that are set. All state agencies and counties must view themselves as both givers and receivers of information, and accept the responsibility that noncompliance by any one entity will jeopardize the overall network. The group governing the CJIN enterprise must be able to set standards and enforce the position that no entity will receive state monies for any effort which fails to meet the minimum standards.

3. The ability to secure incremental funding to meet three fundamental needs. First, there are small counties that simply cannot fund the gap between their current systems and the standards which they will be expected to meet on behalf of the CJIN enterprise. The "buy-in" by these local governments will be in direct proportion to the state's willingness to fund this technological gap. While every county will benefit from the projects recommended in this study, some will benefit more and earlier in the development cycle than others. Those who will not experience the value added benefits immediately should not have to endure financial hardships in the

interim. There needs to be start-up funds to assist these counties as documented in the Section VI - CJIN Project Strategy.

Second, while no system can meet the unique needs of all state and local users, there are local governments that may or will in the future have components of an integrated system in place that may be appropriate to be made available to other locations. Examples include automated jail systems or enhancements to uniform crime reporting systems.

With financial assistance from CJIN, these products, developed with state and local collaboration, could provide an early and tangible sign of the commitment and effectiveness of a statewide network, and form a foundation for the more complicated developments that will be necessary to fully achieve the level of integration in the criminal justice information system needed by the state.

It is important to note that this particular use of funds is intended to maximize the potential of other funds already in place, and is not to replace or duplicate core functions already in place or contemplated at the state level. Instead these funds can accelerate the development of a statewide network using local expertise by targeting funds to appropriate projects. It is fully recognized that local enhancements must be in-line with core functions of state agencies. These funds would not be used to obligate either state or local entities to fund or use the products developed.

And third, there are projects which may have a low value to any one agency or group, but where successful implementation would benefit the entire system (i.e., interoperability of systems). Since individual agencies simply will not make these projects internal priorities, CJIN will need some monies to fund these important interfaces as the group serving as the primary advocate of the criminal justice information system statewide (e.g., the Data Sharing Standards Development project).

Independence Of Agency Management

The CJIN Governance structure is not intended to dictate the organization or operation of any state or local agency, except when dealing with enterprise-wide issues. And, when these CJIN projects are undertaken, frequent communication is necessary to ensure coordination and cooperation between state and local agencies. For instance, in the area of funding, local governments could, with financial assistance from CJIN, serve as pilots for the development and exporting of enterprise-wide projects to other jurisdictions. It is contemplated that such funds would be limited to projects that would deliver a key element of an integrated system. It is expected that funds would usually be used on projects that are clearly the responsibility of the local governments to provide, unless the state agency responsible for the development of the key element joins in the request for funding the project as part of its plans to provide elements of the system by working jointly with one or more local governments.

For projects meeting these criteria, the funds would be used either to finish local development projects that are in progress or to pay the costs of adapting a locally developed product to a more general use or both. If CJIN funds are used, the product developed or adapted would be made available to other users without cost, if the CJIN Board concludes that the final product is appropriate for use by others. If the project is a joint state / local project to develop an element of the system that is solely the state's responsibility, then, of course, the state agency responsible for that element would also need to endorse its export to other users, based on its adherence to CJIN data sharing standards and its consistency with state statutes.

Commitment to Action

The CJIN leadership must be able to convince the General Assembly that support for the CJIN enterprise is an investment of capital similar to the decision to build a prison. While start-up funds and project development monies will be required, there also must be a long-term commitment to a new way of doing business.

One primary consideration must be the realization that state and local agencies already are spending considerable funds on the issues addressed in our recommendations. *The option, therefore, is not whether money will be spent on the criminal justice system, but whether the expenditures will be targeted, coordinated, and designed for the maximum benefit of users statewide.*

For these reasons, in particular, it is critical that the CJIN governance group be approved, established and funded by the General Assembly as promptly as possible. If this is not accomplished in the 1995 legislative session, there will be no visible leadership to direct the development of the recommendations made in this report and to serve as an advocate for the CJIN enterprise. In addition, a delay will cause some state agencies and local jurisdictions to further commit their limited funds to the development and enhancement of systems that do not support an integrated network. Further delays add to the fragmentation of the system, and make future connections even more difficult. And finally, a delay in addressing this issue would send a message to the general public that the state is not serious about moving forward on this issue despite the high level of consensus of users across the state as represented in our findings and recommendations.

Summary

The development and acceptance of a CJIN governance model is central to the overall success of this project. A consensus across the lead state agencies and local agencies on this issue is necessary to gain the political and financial support required, and for the implementation of the specific projects as well. In reaching a successful resolution of this issue, all parties need to recognize and address three realities. First, the legislative creation of a new body or the reconstitution of an existing body will be needed to meet the governance goals of CJIN. While the governance models discussed take into account existing structures, there is no one organization, in its present form, which can or will be endorsed to provide the leadership of CJIN. Second, the governance structure developed will change how existing agencies at both state and local levels function with respect to technology development. While such changes are intended to be minimized, the focus on what is best for users statewide will require individual entities to make policy decisions with an eye toward their impact on agencies outside of their own. And third, the focus at this point should be on the quality of the people selected to serve on the CJIN board and on the scope of the board's role rather than on the myriad of procedural issues which might or might not present problems. If the board has a clear mandate and its members have the respect of the communities served, the procedural issues will be addressed successfully.

Organizational Constraints

One of the challenges involved in introducing and managing technological change is the reality that the tools of technology always exceed the readiness of people and organizations to use them (i.e., what is technically possible is not always socially acceptable). In recognition of this situation, the Change Integration methodology, developed by Price Waterhouse, was used to examine the issues that might inhibit the full and timely implementation of the CJIN Study recommendations. These constraints will be grouped into and presented under three broad categories: individual resistance, institutional barriers, and systemic constraints. The particular relevance of each constraint to this study, along with some recommendations concerning how to reduce or alleviate the constraint, will be included with each level of analysis.

Individual Resistance

All change takes place one person at a time. The common concern of those experiencing the change can be represented best by the question, "is it good or bad for me?" At a more precise level, this question is addressed in relationship to the following four concerns:

- **Feelings of uncertainty** - The fear of the unknown and the inertia which it fosters actually creates a preference for a "bad" known over a "good" unknown. This attitude is captured succinctly in the popular adage that "people prefer the devil they know to the devil they don't." Perhaps no area of innovation fosters this fear more than technological change, which always seems to take longer, cost more, and produce less than was originally promised. To this fear of the unknown must be added the fear of the irreversibility of the technological changes proposed. Since all change is prospective in what it offers, there is an understandable concern that major changes will be made that are not well researched, but then will be continued because heavy investments have been made to achieve them.

- **Sense of loss** - The change process is not unlike the grieving process people experience from a personal loss. The criminal justice culture is known for defending current procedures by the firm assertion, "we have always

done it this way." Although technological change may increase both effectiveness and efficiency, it will accomplish these goals at some costs. Some people could have their jobs changed dramatically or even be reassigned. Others could feel a loss of status or even a loss of control, power, or autonomy over their work. Those that feel they have the most to lose will fight the hardest to maintain the status quo.

- **Threat to personal competence** - A major source of self-esteem for an individual is the ability to perform work in a competent manner. Quite often, however, the need to learn new skills, particularly in the area of technology, serves as a threat to this perceived level of competence and causes people to resist it. The security that comes from knowing how to successfully operate under the current system is replaced with uncertainty and doubts about one's ability to function in an equally effective manner under the proposed system. This concern is exacerbated if there is a lack of training in the use of the new technology, that only serves to further convince people that the old, tried and true system is best.

- **Lack of involvement in decisions** - Most people believe they should have some input into decisions that directly affect their work. In fact, people quite often will even resist a change they agree with intellectually, if they feel they have been ignored in the planning and decision making process. This sensitivity to the lack of direct input into the change process appears to stem from the belief that everyone has a contract (actual or implied) with the organization in which they work and that any change requires an open renegotiation of this contract. This sensitivity is especially acute when technological change is the focus, because the end user of the future technology is so often neglected in the development process.

Consequences for CJIN Project

Since the CJIN enterprise will address issues at both the state and local levels and across law enforcement, courts and correction, literally thousands of individuals working in the system now and in the future will be affected directly or indirectly by the projects proposed. A thorough understanding of how people's work lives will be changed (either positively or negatively in their perception) and a genuine sensitivity to the changes that will occur should be the first prerequisite to dealing with resistance at the individual level. The approach should be one not of minimizing the impact of change, but of legitimizing personal concerns through honest conversations regarding the proposed changes. In this

regard, the initial presentations regarding the proposed changes need to be conducted clearly and in a manner which distinctly separates ideas from actualities. Presenting the facts is always preferable to dispelling rumors. One approach would be to provide the Executive Summary of the CJIN Study to the leadership of each agency involved with the charge to disseminate the document to everyone in their respective organizations. People will hear about the report in pieces anyway, and it would be best to make it a deliberate and positive communication rather than some secret document circulating through the system. A second strategy to deal with this natural resistance, which is addressed in our project recommendations, is to accelerate the implementation of projects that will benefit the individual users, such as the livescan fingerprinting system and a magistrate system. Some early deliverables will build credibility, reduce resistance, and generate the momentum needed to address larger and more complex issues.

Institutional Barriers

The development of a criminal justice information system within a local county or single agency is a major challenge. The development of such a system statewide is a challenge of increased magnitude. While there are a myriad of reasons for this quantum advance in difficulty, there are several institutional factors which are especially pertinent to the recommendations made in this study.

- **Separation of powers** - Any project designed to create or enhance a statewide criminal justice information system will need to both transcend and integrate the missions of the three branches of government. While crime clearly affects each branch and requires a coordinated response, the sovereignty of each branch of government must be preserved in the process as well. This situation is made even more difficult by the fact that there are, and will continue to be, competing priorities for funding between the three branches and by the reality that the judicial branch is totally dependent upon the legislative branch for its funding.

- **State-local relationships** - There is always stress between state agencies that desire uniformity and standardization and local jurisdictions that press for increased flexibility to respond to local needs. The concern at the state level is that there cannot be 100 different systems if any level of integration of current and future criminal information databases is to occur. At the local level, the primary fear is that they will be forced to

accept an imperfect system with no local control over the decisions. This issue is even more serious in those counties that have already made significant investments in their local information systems. Their concern is that the "new and improved" system will actually provide them with something less than they already have in the name of conformity.

- **Political factors** - Despite the fact that many of the criminal justice stakeholders are centralized administratively, the power of local politics is still a major constraint. The elected officials (sheriffs, judges, district attorneys, clerks, county commissioners, and city councils) all have agendas that reflect the needs of their respective organizations, but may not benefit the system as a whole, and the ultimate power to hold at least portions of the CJIN enterprise hostage through non-cooperation with respect to policy development and / or funding. In addition, there are major differences between the larger urban areas and the smaller rural communities, the latter represent the majority of the counties in the state. The significance of this situation is that many of the advantages of the proposed CJIN enterprise will accrue initially to the larger counties with the more severe problems. If the smaller counties do not see themselves as both givers and receivers of information and / or are not willing to support development efforts piloted in the larger counties, the needed political consensus at the state and local levels will not develop. And finally, in this area, there is the political uncertainty associated with the recent elections. Much of the State's political leadership is new and has not had time to study many of the issues addressed in the CJIN study. Their political philosophies will be revealed over the coming months, but it is difficult to ascertain at this point, the strength of their commitment to the recommendations proposed.

Consequences for the CJIN Project

Because the CJIN enterprise crosses all three branches of government and will require the cooperation of each entity to succeed, the major issue for this project is the construction of a governance structure for CJIN (as presented previously) that provides for an equitable distribution of power, while preserving the sovereignty of each branch to manage its own internal affairs without intrusion. In addition to the governance structure, it will be important that standards be set statewide and that the funding authority of the General Assembly be used to assure compliance with these standards. If a state agency or local jurisdiction is permitted to develop a local product that compromises the overall system, this tolerance will quickly compromise the primary goal of an integrated system statewide.

The relationship between state and local agencies is equally important, but perhaps somewhat easier to address. The goal of the CJIN enterprise is not to develop a centralized state system that dictates operational policies to local jurisdictions. Rather, the vision for the CJIN enterprise is to meet the statewide information needs of local jurisdictions. The focus of each of the recommended projects, therefore, is to address those areas of activity where there is a clear and functional interdependence between counties and between counties and state agencies. Local jurisdictions will need to be shown early and often that the true goal of the CJIN enterprise is to enhance local operations and not to extract information from them in support of efforts that have no local value.

In response to the current political culture, several strategies should be considered to minimize the constraints. First, counties with portions of the CJIN enterprise already partially or fully developed should be targeted as "best practices" sites and their work should be completed or refined for prompt export to other counties, especially the smaller ones where funds for development and staff expertise simply do not exist. This approach would establish early on that the work done by local jurisdictions is respected and it would provide a peer or user-to-user model for developing the system statewide. Second, funding at the earliest stage should be targeted for counties whose current systems do not meet the proposed standards. In essence, the goal would be to close the technological gap so that all counties could participate in the basic elements of the new system. Not only would this approach provide practical assistance, but it also would mitigate the tension between political officials at the state and local levels. And third, there needs to be a strong marketing (not selling) effort with the General Assembly to stress both the importance of a statewide criminal justice information network and the practical advantages for all counties of the projects recommended. This marketing /

educational effort should involve representatives of the users at both the state and local levels to demonstrate the "grassroots" level of support for this effort and to thereby give all political representatives a reason for supporting it.

Systemic Constraints

In addition to the above issues associated directly with resistance at the individual and institutional levels, there are three other areas of concern that, if not addressed early and in a deliberate manner, could compromise the project. These areas are funding conflicts and limitations, statutory and policy constraints, and the lack of system-wide education and training.

- **Funding issues** - Although the projects recommended for initiating the CJIN enterprise focus on the needs of all counties and the agencies representing law enforcement, courts and corrections, the needs of the criminal justice system represent just one of many issues which will compete for scarce dollars at the state and local levels. This issue is complicated further by current efforts to reduce the size of state government and the associated costs. For those agencies currently represented for funding purposes through the AOC, there is the issue of whether all funding for the CJIN enterprise that affects these agencies should flow through the AOC, directly to the counties or in some combination. Also, there is the reality that some counties simply cannot afford even the most modest level of capitalization required for them to be able to connect with and access information from other counties or state agencies. Many of these same counties do not have the staff, or the staff with the expertise, to implement the projects proposed. In addition, there is the issue of how to generate revenue, beyond traditional government funding, to support the CJIN enterprise initially and, just as importantly, over the long term. And finally, there is the issue of whom should control the funds made available for this project to assure compliance with the standards that priority projects receive the preferential funding required for success.

- **Statutory and policy constraints** - These issues fall basically into the categories of confidentiality, access, and local legal culture. With regard to the first area, the current statutes governing the confidentiality of juvenile and mental health records represent the most widespread concerns. With respect to juvenile records, the primary difficulty is the lack of access to the juvenile's criminal history for law enforcement and with respect to structured sentencing, for the district attorney. In a similar fashion, mental health records are closed even as they

relate to involuntary commitments. Law enforcement would like access to this information, which would not require access to treatment information. In a similar vein, information maintained by the Department of Revenue (i.e., previous drug events) and the Employment Security Commission (i.e., employment history) also is currently protected and unavailable for use by the criminal justice system.

While not statutory, there are historical practices at the state and local levels that have come to characterize the local legal culture that, unless changed, will limit the effectiveness of some of the recommendations. For example, the potential for electronic warrants will have to address the current commitment to the possession of a hard copy document by law enforcement officers at the time of arrest. In general, the system is document oriented and efforts to reduce paper will have to overcome this constraint. At the operational level of each agency there are long standing practices that have defined the role of the various participants and how work is processed. A relevant example here is the possibility of "real-time" data entry in the courtroom that would provide immediate access to the court's decisions, but would require a different pace of case management for judges and the courtroom clerks. At present, it is not uncommon for a defendant to be sentenced and then remain in jail for a week waiting for the paperwork to be signed and forwarded to the DOC. There are a myriad of these situations that technology could alleviate, if the people involved would be willing to change long standing practices.

- **Lack of systemwide education and training** - Even though efforts should be made to use and enhance existing systems with which people are already familiar, new skills and procedures will be required to implement the proposed projects. For the counties with existing networks, this disruption will be one primarily of time, rather than of expertise, but it will result in some resistance. For the counties with no existing system and / or staff skilled in the use of the technology involved, the impact will be considerable, both in terms of the time required for training and for the recruitment and training of qualified staff. If training on the statewide system for both types of users is not a priority, the system will be compromised in its overall use and with respect to the accuracy with which important information is managed. These negative outcomes would affect both the local jurisdiction as well as users statewide.

Consequences for CJIN Project

The funding model developed in support of this project, along with the related governance structure, is the ultimate key success factor. In the development of this model two issues should be emphasized. First, a great deal of taxpayer dollars have and will continue to be spent on criminal justice information systems. And, while there is considerable evidence that individual agencies and local jurisdictions have added value to their work through these expenditures, the system statewide has not been a primary beneficiary. However good individual systems are, they have developed on an ad hoc basis with little attention paid to compatibility and access statewide. Any additional funds spent in this manner will only increase this problem and make future efforts to achieve an integrated system that much harder and that much more expensive. Those making the funding decisions must realize that the issue is not whether funds will be spent, but whether they will be spent to develop an integrated system that meets the broad needs of the criminal justice community.

The second issue relates to the need for long-term funding. While there will need to be a considerable infusion of capital for start-up costs, this funding, without a commitment for funding over the next five to ten years, will result in a crippled and unfinished system. One of the classic mistakes made by other states has been to fund the initial purchase of equipment with no follow-up support for system maintenance and enhancements and training. A statewide criminal justice information system should be viewed in the same way as a capital investment in a prison (i.e., it is for decades and not years). While this approach to funding is counter to the state's two year budget cycle, a two year frame of reference simply will inhibit the development of the system and break the continuity of the process. In addition, it will delay budget decisions at the local level, because it will be difficult to know what the state plans to do, if anything.

Even if the above two issues are addressed, it is not assumed the state can fund the entire system. Additional revenues will be needed and these should come from several sources (including counties), but especially from the defendants who enter the system as well as from external agencies who use the system (e.g., insurance companies, professional licensing boards, employers). And, if there is a cost (user fee) to the internal users, this cost should be equitable and prorated on actual usage. It should also be recognized that those counties with existing pieces of the system must accept the responsibility of exporting their current systems, or those developed with funds targeted to the CJIN enterprise, to those counties that do not have and cannot afford such development costs. This willingness to help subsidize other counties must be recognized as a cost that will benefit everyone.

The constraints that result from existing legislation or from agency practices must be reviewed in light of the needs of the overall system and not narrowly on an agency by agency basis. Statutes should keep pace with technology and the need to access previously closed databases, with appropriate safeguards, has to be a discussable topic. For example, the nature of juvenile crime has changed. The increase in violence and the use of firearms warrants a review of the confidentiality statutes that keep law enforcement agencies from accessing a juvenile's criminal history. The strategy in any area of confidentiality (e.g., mental health, income tax, employment, juvenile) should be to look at the purpose and the merits of the request for such information, assess the risks to law enforcement and the public from not having access to such information, determine the ability to provide safeguards to abuse, and then weigh the merits of the existing legislation.

The strategy or approach to dealing with the local legal culture is difficult as well, since there is no clear statute to evaluate or standard practice statewide in these multiple areas. Each local agency has their practices that work for them. What will probably be needed is an evaluation of each CJIN project adopted to determine the current business practices which need to be modified to obtain the full value of the technology available. Some of this will be driven by the development of statewide data and communications standards, but there will be many local practices that need to be revised to achieve full effectiveness.

The final topic in this section deals with the need for statewide education and training. As important as it is to fund the hardware and software required, if funds are not also available to train people how to use them, the system will falter. The key strategy here is to train the people who will actually use the system and to begin training them on projects that will have the most value for them in their daily work and where they will see the clearest results. Depending on the vendors selected, it may be appropriate to have the vendor contracts include the basic training component. If the decision is to stay internal, the strategy should be to create teams of trainers which include local users as well as those expert in the system statewide. Local users are already anxious about the changes technology will require and their ability to learn the new systems. This anxiety would be reduced if peers with whom they can identify are involved in the initial training phase.

Summary

The overall intent of this entire discussion is to sensitize policy makers, and those responsible for the future implementation, to a set of issues that are known to have a dramatic and direct effect on the success of any technology project. While the substantive merits of any proposal must be established, the intellectual recognition that the recommendations are warranted does not lead automatically to successful implementation. A good idea is a necessary, but insufficient ingredient in bringing about change.

Technical Strategy

The following sections present a discussion of the key technical components that comprise the overall CJIN strategy and standards. Our recommendations adhere to IRMC standards where they exist. We recommend that these strategies form the foundation for future projects beyond those identified in this report. These strategies include:

- ***Data Management***

A description of strategies to facilitate the exchange of data in the criminal justice arena including data standards, data capture, database management systems, reengineering and development tools, data warehousing, and data archiving.

- ***High Level Enterprise Data Model***

A description of the CJIN enterprise data model and how it changes as the recommended projects are implemented.

- ***CJIN Network Architecture***

A description of near and long-term systems strategies for integrating criminal justice information systems, including hardware platforms and configurations, software applications, operating systems, utilities and support, peripherals, network communication protocols, interfaces, and standards.

- ***CJIN Security***

An analysis of security issues as they relate to the accessing and sharing of criminal justice information, including authorization, authentication, encryption, and public access.

Data Management

This section provides an overview of the data management strategy necessary to facilitate the exchange of information in CJIN. The strategy will define terms and make recommendations for implementing data management in CJIN.

Overview

Data management is the control of information from its introduction to the enterprise to its final point of use.[1] *Information is a resource as valuable to the criminal justice network as money, people, and equipment.* The importance of this resource and the rate of its growth create the need for a management strategy to guarantee users access to timely, reliable, and accurate information. The CJIN data management strategy provides this assurance by controlling the capture, definition, ownership, identification, retention, and archival of statewide criminal justice information.

CJIN data management strategy makes recommendations for:

1. Data Standards
2. Data Capture
3. Database Management Systems
4. Data Reengineering and Development Tools
5. Data Warehousing
6. Data Archiving

[1] Dictionary of Computer Terms, Charles E. Puffenbarger, 1993 Barnes & Noble

1. Data Standards

Recommendation

Develop a statewide data dictionary to standardize all facets of repository information.

Explanation

The CJIN Study identifies a priority project to develop a statewide data dictionary. A data dictionary collects and documents metadata. Metadata is information describing the data elements stored in CJIN databases, or data about data. Metadata in the dictionary describes entities and attributes. Entities are a set of information, usually about a single item. A victim is an example of an entity. Attributes are data items that describe an entity. For example, a victim has a name, address, sex, race, and date of birth among other attributes. The dictionary will promote the sharing of information among all network databases by driving the development of common definitions for entities and attributes. *The most significant current inhibition to data sharing is the lack of common definitions, formats, and identifiers of data entities and attributes.* The dictionary will analyze, centralize, and document data management of entities and attributes.

Entity

An entity consists primarily of the following items:

- Name
- Aliases
- Description
- Identifier
- Custodial Organization
- Attributes

The following points explain the information necessary to standardize or record for the components of an entity:

- *Capture all names and aliases of a data entity*. Data standardization becomes critical at the entity level. The dictionary collects all names and aliases for an entity. Each agency can refer to the information in its own terms. For example, organizations refer to a person by many titles throughout the justice process: suspect, arrestee, defendant, inmate. Through entity names and aliases, the dictionary captures all labels for a data group. The dictionary acts as a roadmap allowing a user to find the data by any name in any CJIN database.

- *Capture a single, common definition of an entity description.* For example, a criminal case history to the State Bureau of Investigation (SBI) consists of all felony and some misdemeanor offenses connected to a person based on fingerprint identification. However, to the Administrative Office of the Courts (AOC), criminal case history consists of both felonies and misdemeanors and is not necessarily linked to a person by fingerprints. The common definition of a criminal case history must be developed to facilitate data exchange. The CJIN Study Report discusses this example in the Statewide Criminal History Repository Project.

- *Define a single, unique identifier for each entity*. Entities must contain at least one identifier. The identifier is the primary method to find a single occurrence of an entity. The identifier is the index, or pointer of a database. The network model and the distributed computing environment are dependent upon the proper definition of

entity identifiers. Each entity should define a unique identifier used by all agencies to insure the accurate reporting of the information requested. For example, when searching the database by name, which is an inexact search, the database can return a candidate list, but when searching by State ID (SID), the database can return an exact match. The SBI / DCI and AOC are currently implementing an interface to populate both the check digit number and SID number in both databases. The Department of Correction identifies a person by the FBI number, but is planning to implement the SID. The effort to promote common personal identifiers is the basis from which to build the statewide data dictionary and common identifiers for all shared entities.

- *Define the custodial organization for an entity.* As CJIN eliminates data redundancy and streamlines the network, issues of data management become more critical. As a rule, *the agency responsible for the function that creates the entity becomes the custodial organization for that entity*. Along with the committee responsible for the data dictionary development and adoption, the custodial organization assumes management responsibility for the data element. The responsibilities of the custodial organization include cooperation with the CJIN governing body for:

  - Quality assurance of the information.
  - Standards adoption.
  - Interaction with other agencies in response to changing information needs.
  - Coordinate resolution of further definition and usage conflicts.

  The custodial agency is also responsible for naming a knowledgeable individual as data custodian, whose responsibilities include:

  - Acting as a functional expert in the use of the entity.
  - Reviewing metadata changes.
  - Reviewing use changes.
  - Participating in conflict resolution meetings on entity usage.

Attribute

The components of a data attribute definition include:

- Name
- Aliases
- Description
- Length
- Properties
- Valid Values
- Stewardship

The following points explain the information necessary to standardize or record the components of an attribute:

- *Capture all names and business aliases for an attribute.* The attribute is the lowest level at which we define data. It represents a single unit of information such as last name or date of birth. Like at the entity level, the dictionary can capture and refer to an attribute by all of the names and aliases by which it is known. This information promotes sharing by allowing a user to refer to an attribute by a familiar name. But to make the network environment a reality, each user group must agree on description, length, properties, and valid values.

- *Agree upon a standard, common description of the attribute.* As in entity descriptions, agreement upon a single, common attribute definition is essential to the data standardization project.

- *Standardize attribute format.* Length, properties (numeric or alpha), and valid values combine to become the format of an attribute. Length and valid values are most important in debating the adoption of common codes. Each criminal justice agency developed its own codes and associated values for items as diverse as eye color, vehicle make, and statutes, among hundreds of others. Data sharing requires that agencies resolve code differences. This is a large task as many systems' processes are dependent upon specific code values. But from a state perspective, standardization is paramount. National standards should be adapted to fit state needs where

possible. In all cases, standard code use should be mandated, financial assistance should be offered, and transition time set aside.

- *Delineate and assign responsibilities of attribute ownership*. Agencies responsible for the function that adds the entity become the custodian of that entity. That agency must assign a steward for each attribute as well as a custodian for the entity. The steward is responsible for maintenance of the valid data values. The steward:

  - Maintains all global tables.
  - Ensures all attributes receive values in a timely and accurate manner.
  - Implements security requirements allowing or restricting access to specific data values.
  - Participates in conflict resolution for the use (create, update, read, or delete) of an attribute value.

2. Data Capture

Definition

Data capture is the collection of information that is important to the operation of the enterprise. For the CJIN Study, data capture is synonymous with the user interface, or application a CJIN user employs to enter data.

Recommendations

- Do not centralize the development of user interfaces.
- Standardize interfaces through general guidelines, but do not jeopardize the critical development of data standards by attaching interface standardization to the data dictionary development.
- Monitor industry's development of both defacto and formal open system interface standards.

Explanation

Standardizing data across databases eases the communication between systems from a technical aspect. However, standardization of the user interface is also important. The most uniform application interface option is to use one piece of software throughout the network. Unfortunately this option would not only recreate existing applications and infringe on the autonomy of each participating agency, it would greatly increase the needed expenditure for new application development. Short of developing a single application, the CJIN user community should develop and enforce standards for the user interfaces. Best stated in a focus group, "A PF5 on one system should do the same thing as a PF5 on another system."

Standardization of application programs increases importance in the client server environment as the use of graphical user interfaces exponentially increase screen variations. The identification, approval, and administration of user interface standards should not be performed as part of the data dictionary development. The data standardization task is of utmost priority to the success of the network and should focus on the accurate population of data attributes. Individual agencies remain responsible for the development and standardization of user interfaces. However, the CJIN governing body should monitor the continuing development of standards by groups such as the Institute of Electrical and Electronic Engineers (IEEE), Open Software Foundation (OSF), and other proprietary standards. Recommending a standard today would be unwise as no one direction has significantly captured the open systems, user interface development market.

3. Database Management System

Definition

Database management systems (DBMS) provide for the storage, manipulation, and administration of interrelated data stored on computer accessible media.

Recommendations

- Each organization migrates to a relational database management system.
- The network connects the relational database management systems using a distributed database management system under the framework of the Open Software Foundation's Distributed Computing Environment (OSF DCE).
- Utilize enterprise gateways to access the data in diverse databases.

Explanation

All systems must begin migration toward relational database management systems. Relational systems allow the highest level of flexibility in data structure changes by separating the physical data structures from programs. Technical participants in focus group sessions agreed that all state repository data must begin to migrate to a relational environment.

Overall, CJIN is best served by a distributed database management system. The distributed systems will link agencies' relational systems and allow user queries to pull together data from many databases to form a concise view for the user. One query may return a single list for the user combining data from the SBI, AOC, DOC, and other databases. A tool recommended for accessing multiple databases and defining custom user views to information from diverse platforms is the enterprise gateway. Figure V-1 displays the gateway principle. Each agency could implement a gateway that accesses the data needed for specific user needs. Development of the data dictionary can facilitate writing applications for the gateways. Items such as data location, ownership, and format can drive the gateway application.

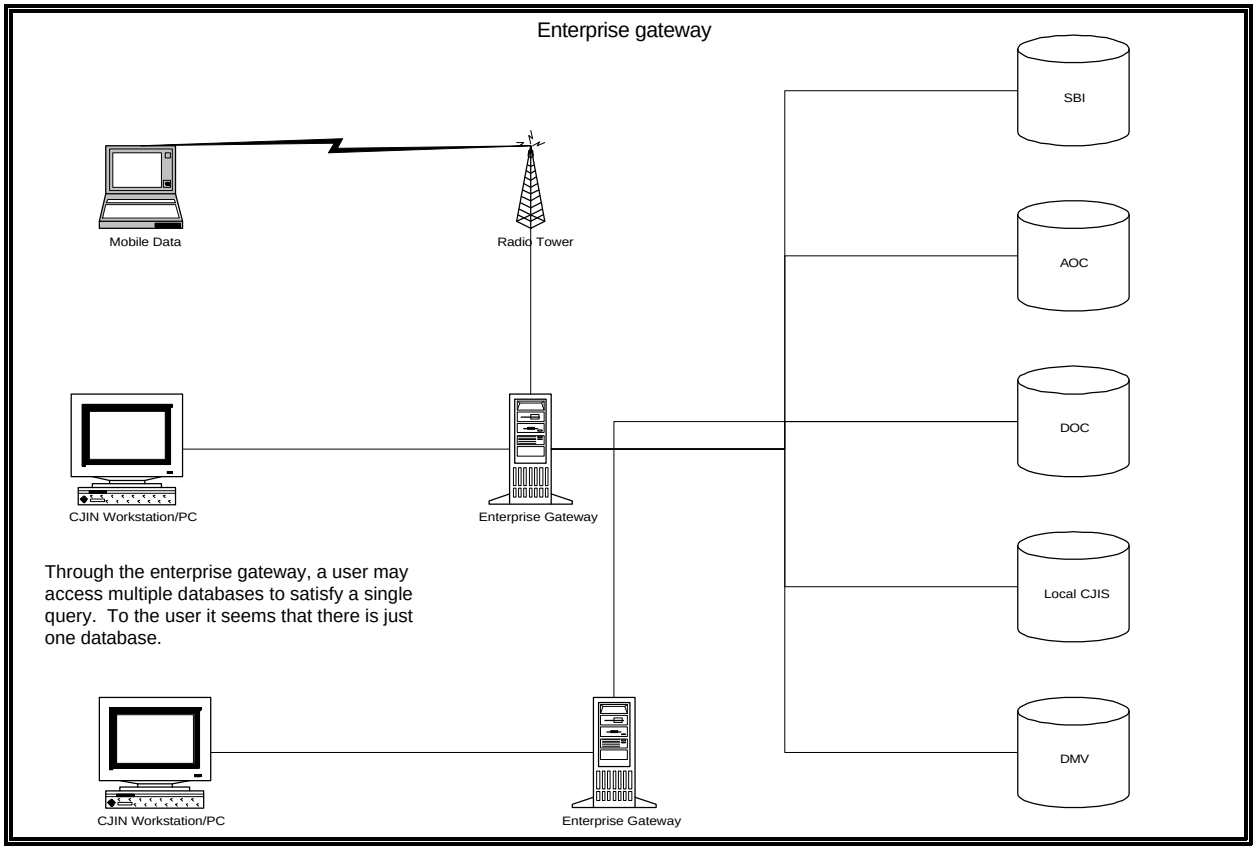

Enterprise gateway
SBI
AOC
DOC
Local CJIS
DMV
Mobile Data
Radio Tower
CJIN Workstation/PC
Enterprise Gateway
Through the enterprise gateway, a user may access multiple databases to satisfy a single query. To the user it seems that there is just one database.
CJIN Workstation/PC
Enterprise Gateway

Figure V-1

4. Data Reengineering and Development Tools

Definitions

Data reengineering is the process of using existing data structures to:

- Improve understanding of the information stored.
- Reconstitute the information to meet needs that are currently unmet.

Existing data structures drive the development of target data structures on modernized platforms to increase the reuse and evolvability of the software. Development tools can assist in the process of database and application documentation and generation.

Recommendations

- Reengineer the data in transition from legacy to relational architecture.
- Use Computer Aided Software Engineering (CASE) tools to perform the migration to relational architectures.
- Do not mandate the use of specific tools. Allow agencies that fit their trained base of developers and unique transition needs.

The migration to relational and distributed platforms facilitates a need for data and system reengineering. Reengineering will be necessary for each agency as it moves to a new environment. Most agencies have already realized this cost, such as the DOC in the development of Offender Population United System (OPUS) in a DB2 relational structure, or the AOC's plans to reengineer their Court Information System (CIS) system.

Moving toward a relational, distributed environment, all participating agencies can benefit in using the tools available to develop applications on multiple platforms. Current generations of CASE tools allow common procedures to be written and shared by applications that can be ported or moved to multiple environments. The use of CASE technology and leverage of existing systems minimizes the expense of extensive data reengineering.

There is no need to mandate data reengineering tools or techniques to CJIN agencies. Migration to a relational database management system should be a CJIN goal, but the tools and techniques should remain the jurisdiction of individual organizations.

5. Data Warehousing

Definition

Data warehousing is an architecture designed to manage large amounts of data. The concept separates data into varying levels of detail and provides that information to users depending on specific needs. Often, data warehousing introduces redundancy by adding a summarization level for decision support.

Recommendations

- Adopt concepts of data warehousing that fit the goals of CJIN. These include:

    1. Detailed documentation of metadata.
    2. Provision of a summary layer in the Statewide Identification Index that provides a snapshot of summary data.

- Do not allow warehouse concepts such as multiple detail layers drive the development of the network. Concentrate on standardization and connectivity rather than detail granularity.

Explanation

Data warehousing is a concept being adopted by many organizations. The technology promotes using information detail to make short-term decisions and the summarization of data to influence long-term decision making. Warehousing often collapses data past a certain age into summarization. In addition, it adds summarization levels redundantly over existing data structures for decision support. Key concepts of data warehousing are proposed in CJIN transition projects. The development of the data dictionary, the summary location and demographic information in the Statewide Identification Index, and gateway access to distributed databases all have foundation in data warehousing. But aged information in a statewide criminal justice system does not lose its importance to decision making. Comprehensive criminal history includes older events or episodes at the same level of importance as new ones.

Allowing CJIN development to concentrate too heavily on implementation of complex warehouse structures could negatively impact the development of the network. Key factors such as data standardization and connectivity should drive development.

VI. Data Archival

Definition

Data archival involves the removal of information from the direct online access databases. Data is either stored off-line or in computerized databases that are not required to meet immediate access requirements.

Recommendations

- Define the length of time a data element must be available for immediate access as part of the data dictionary exercise.
- Continue to manage data archival per agency but mandate that archival meet retention requirements defined in the data dictionary.
- Allow computer system performance requirements to drive the necessity for archival rather than the cost of on-line storage.
- Utilize compressed, computerized storage of archived data.

Archival requirements define the length of retention of information in the primary computerized database. Each organization currently defines and manages its data archival requirements. In defining metadata for each attribute, the participants in the development of the data dictionary should document their retention needs based on statutes; federal, state, and local requirements; and business operations. For example, retention of criminal history must meet structured sentencing requirements, the guidelines set by the Federal Bureau of Investigation, National Crime Information Center's Advisory Policy Board, and the business needs of each justice agency. The greatest denominator should become the on-line retention length.

Once the dictionary defines retention, archival should be left to the custodial agency for each entity. If possible, the custodial organization should maintain the information on-line as long as system performance is not downgraded. An agency's choice of archival method should not be mandated. As magnetic storage and data compression technologies advance, the cost of maintaining computerized archive files should continue to decrease.

High Level Enterprise Data Model

A data model is a graphical representation of the information stored by an organization. At its highest level, a model shows the interrelation of databases and other large groupings of information between agencies. At its finest level of detail, a model can display structure and relationships of every entity about which the organization stores information.

This section contains iterations of a High Level Enterprise Data Model. This model assumes an enterprise perspective to show the storage of data in CJIN. The purpose of the high level data model is to examine the interrelationships between information across agencies, and to organizations external to CJIN. This section contains a number of "snapshot" models. The first, the current databases, depicts the model as it exists today. The current model is a base from which to begin transformation. Subsequent "snapshots" redisplay the impact of key CJIN development projects on the databases. The final model depicts the target CJIN database, one that through a distributed database management system and / or enterprise gateways, appears to the user as a single database.

Approach

The model consolidates information from many sources. The approach includes the following inputs:

- *Focus Groups.* In many focus groups, participants diagramed current and desired information exchanges between databases. These exchanges formed the basis of the current and future models.
- *Database Documentation*. Database schema diagrams and layouts from the SBI, AOC, DOC, and DMV both confirmed and augmented the current model.
- *Public Forums*. Public forum comments helped in completing both the current and future data models.
- *Stakeholder Interviews.* These interviews provided a view of the future needs of CJIN. The target model structure supports these needs.

- *DBA and Application Administration.* Database and Application Administrators provided essential information in many focus groups. These are the people closest to the data, and they provided valuable insight into the enterprise needs to maintain certain data elements.

- *National Publications*. Specifications of NCIC-2000 and Bureau of Justice Statistics manuals guided the transition to the target architecture. The target design allows North Carolina to meet identifiable future requirements and the flexibility to meet unforseen needs.

Current CJIN Databases

Figure V-2 represents data subject areas in the current database environment. A subject area is a grouping of like entities and attributes. Subject areas allow a data model to display high level representations of information without forcing debate of data normalization and other design concepts.

Beyond subject areas, the figure also depicts communications and external interfaces. These items are not included to show redundancy or other concerns in the current data structures. Instead, these items are included to document external interface requirements that must remain in the target data structures.

Each box in Figure V-2 represents a grouping of systems (manual and computerized) and databases owned by a specific organization. Each of the following diagrams display the role key CJIN projects play in creating the view of one database for the user community. Many system additions will span horizontally across the diagram showing access to the information by all authorized users regardless of their organization or physical location.

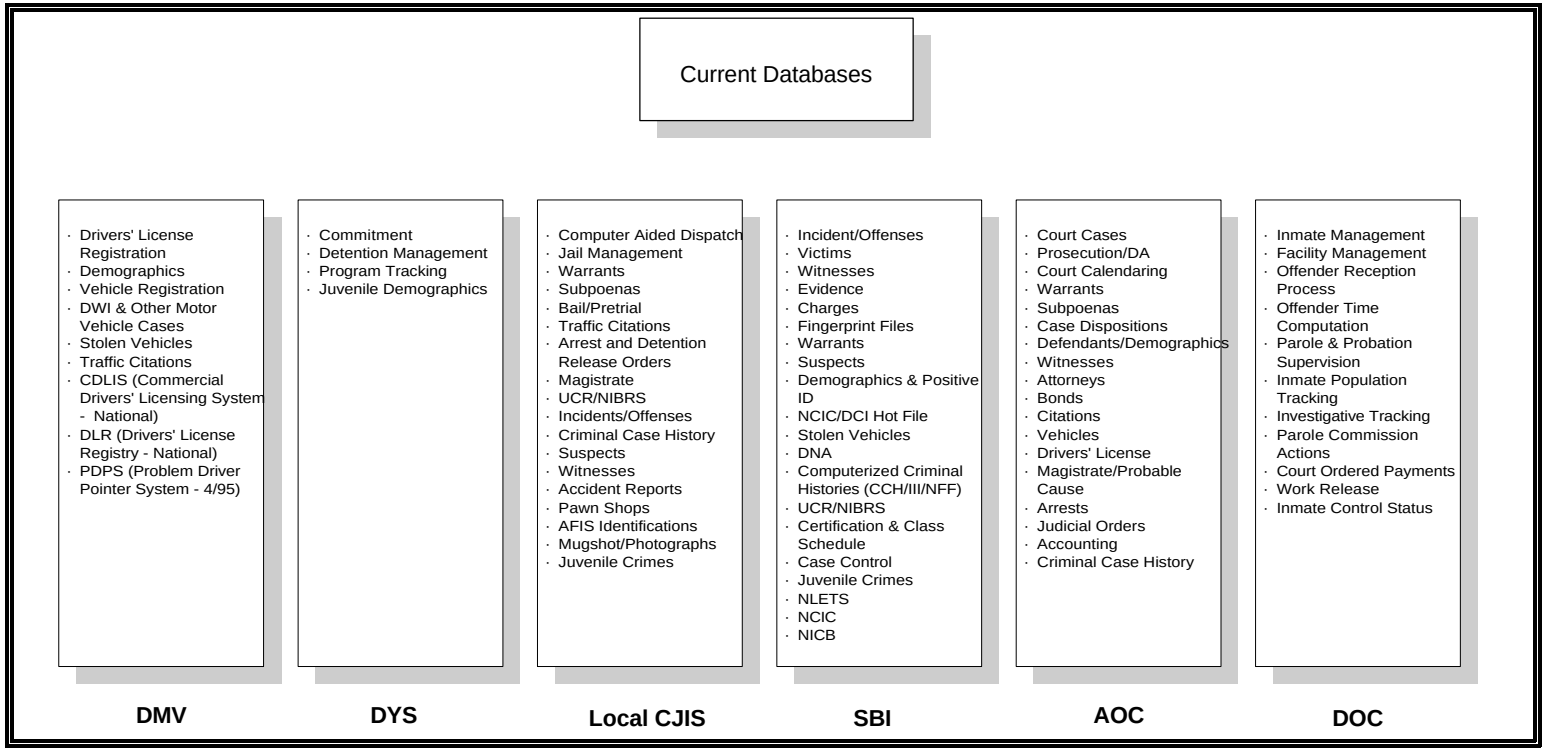


Figure V-2

Concerns of the Current Database Environment

- CJIN organizations currently maintain autonomous databases which are loosely connected by interfaces that pass information. One example is the check digit number, a unique identifier of an event or episode assigned at the point of fingerprinting. This information is passed between law enforcement, SBI / DCI, and AOC to reconcile case disposition.

- Data is unnecessarily redundant. Subject areas such as personal demographics, vehicle information, and criminal case history exist in multiple databases.

- There is no method to decide which information is most accurate. A network program can access data on multiple databases. However, in the current CJIN environment the program could not determine which of the redundant information is correct. In addition, no summary level information currently exists. For example, should a user ask the network to show the current address of a person in custody, the program would not only have to return multiple people from whom to choose, it would have to return multiple addresses not knowing which database contains the "best" information.

- There is no data element that indiscriminately connects events or episodes across multiple databases. The check digit number makes the connection for fingerprinted offenses, but non-fingerprinted offenses cannot be associated. The options are to use another unique cycle tracking number for non-fingerprintable offenses or to increase the fingerprint activity to include misdemeanors.

- There is no common personal identifier used by all agencies. Some organizations use the LID (Local Identification number) or SID (SBI / DCI's fingerprint based State Identification number), but the DMV uses a different identifier and the DOC uses the FBI Identifier. To facilitate the sharing of personal records and criminal history, all criminal databases must adopt the SID.

- Redundant data entry consumes valuable resources and damages the reliability and timeliness of the data.

- In areas such as court case disposition or stolen vehicle recovery, an update to one database is immediate while an update of another is weeks to months behind.

- Data passed between agencies does not have a common code or identifier basis. For example, agencies use different codes for demographic information, offense codes, and unique event or episode numbering.

- Database architectures are not flexible in meeting changing local, state, and federal requirements.

CJIN Network Security Project, End User Technology Upgrade Project, TCP/IP Communications Implementation

Figure V-3 reflects the CJIN databases after the completion of the CJIN Network Security Project and implementation of the End User Technology Upgrade Project and TCP/IP Communications. The security project facilitates network data access through standardization of the security profile. Access to juvenile information will require a higher level of authorization contained in the profile. But the software security mechanism will be the same as implemented in adults' records.

The End User Technology Upgrade and TCP/IP projects combine to begin to break down the technical barriers between systems and databases. By completing these projects the technical infrastructure will be in place to perform interagency, high-speed data communication. Increased connectivity between systems is represented in Figure V-3 by the partial removal of the barriers between systems. Further breakdown of these barriers occurs in implementation of the Data Sharing Standards Development Project.

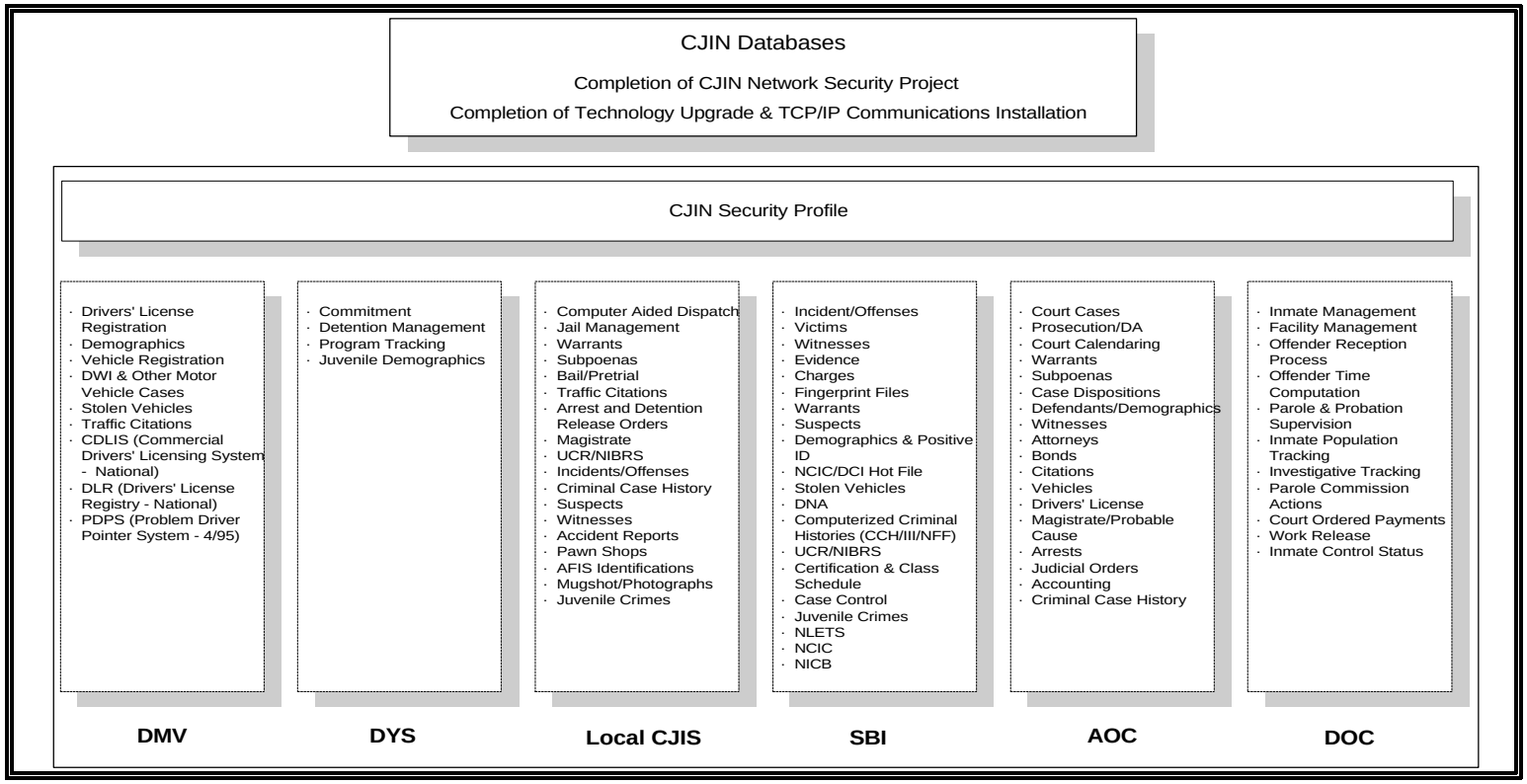

CJIN Databases
Completion of CJIN Network Security Project
Completion of Technology Upgrade & TCP/IP Communications Installation
CJIN Security Profile
· Drivers' License Registration
· Demographics
· Vehicle Registration
· DWI & Other Motor Vehicle Cases
· Stolen Vehicles
· Traffic Citations
· CDLIS (Commercial Drivers' Licensing System - National)
· DLR (Drivers' License Registry - National)
· PDPS (Problem Driver Pointer System - 4/95)
· Commitment
· Detention Management
· Program Tracking
· Juvenile Demographics
· Computer Aided Dispatch
· Jail Management
· Warrants
· Subpoenas
· Bail/Pretrial
· Traffic Citations
· Arrest and Detention Release Orders
· Magistrate
· UCR/NIBRS
· Incidents/Offenses
· Criminal Case History
· Suspects
· Witnesses
· Accident Reports
· Pawn Shops
· AFIS Identifications
· Mugshot/Photographs
· Juvenile Crimes
· Incident/Offenses
· Victims
· Witnesses
· Evidence
· Charges
· Fingerprint Files
· Warrants
· Suspects
· Demographics & Positive ID
· NCIC/DCI Hot File
· Stolen Vehicles
· DNA
· Computerized Criminal Histories (CCH/III/NFF)
· UCR/NIBRS
· Certification & Class Schedule
· Case Control
· Juvenile Crimes
· NLETS
· NCIC
· NICB
· Court Cases
· Prosecution/DA
· Court Calendaring
· Warrants
· Subpoenas
· Case Dispositions
· Defendants/Demographics
· Witnesses
· Attorneys
· Bonds
· Citations
· Vehicles
· Drivers' License
· Magistrate/Probable Cause
· Arrests
· Judicial Orders
· Accounting
· Criminal Case History
· Inmate Management
· Facility Management
· Offender Reception Process
· Offender Time Computation
· Parole & Probation Supervision
· Inmate Population Tracking
· Investigative Tracking
· Parole Commission Actions
· Court Ordered Payments
· Work Release
· Inmate Control Status
DMV
DYS
Local CJIS
SBI
AOC
DOC

Figure V-3

Data Sharing Standards Development

This project will develop and implement a data dictionary. Figure V-4 shows that after completion of the standardization project, boundaries between databases will continue to fall as application programming interfaces (APIs) and common data views are developed. To a user, agency and location of the data becomes less important as CJIN becomes one logical database. The logical database is represented in the diagram by the removal of database boundaries and agency names from specific data stores. The data is represented as one view to the users, but this does not imply that all information will be combined into a central CJIN database. To create one logical view, systems will be built upon common data definitions and will share common codes. Further consolidation and networking of the databases will depend upon standards development. Projects directly dependent upon the dictionary development will insure criminal history accuracy and timeliness, sharing of warrant information, and elimination of data entry redundancy.

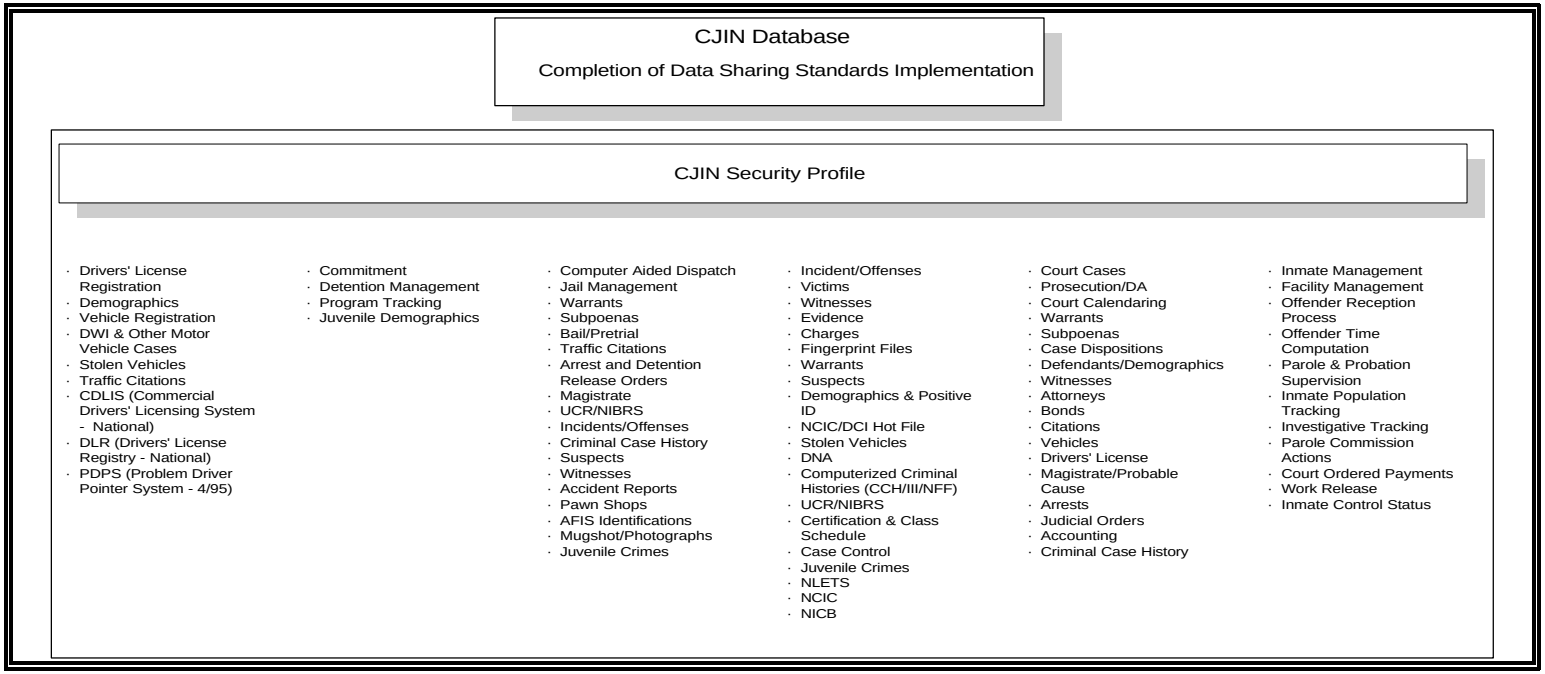

CJIN Database
Completion of Data Sharing Standards Implementation
CJIN Security Profile
· Drivers' License Registration
· Demographics
· Vehicle Registration
· DWI & Other Motor Vehicle Cases
· Stolen Vehicles
· Traffic Citations
· CDLIS (Commercial Drivers' Licensing System - National)
· DLR (Drivers' License Registry - National)
· PDPS (Problem Driver Pointer System - 4/95)
· Commitment
· Detention Management
· Program Tracking
· Juvenile Demographics
· Computer Aided Dispatch
· Jail Management
· Warrants
· Subpoenas
· Bail/Pretrial
· Traffic Citations
· Arrest and Detention Release Orders
· Magistrate
· UCR/NIBRS
· Incidents/Offenses
· Criminal Case History
· Suspects
· Witnesses
· Accident Reports
· Pawn Shops
· AFIS Identifications
· Mugshot/Photographs
· Juvenile Crimes
· Incident/Offenses
· Victims
· Witnesses
· Evidence
· Charges
· Fingerprint Files
· Warrants
· Suspects
· Demographics & Positive ID
· NCIC/DCI Hot File
· Stolen Vehicles
· DNA
· Computerized Criminal Histories (CCH/III/NFF)
· UCR/NIBRS
· Certification & Class Schedule
· Case Control
· Juvenile Crimes
· NLETS
· NCIC
· NICB
· Court Cases
· Prosecution/DA
· Court Calendaring
· Warrants
· Subpoenas
· Case Dispositions
· Defendants/Demographics
· Witnesses
· Attorneys
· Bonds
· Citations
· Vehicles
· Drivers' License
· Magistrate/Probable Cause
· Arrests
· Judicial Orders
· Accounting
· Criminal Case History
· Inmate Management
· Facility Management
· Offender Reception Process
· Offender Time Computation
· Parole & Probation Supervision
· Inmate Population Tracking
· Investigative Tracking
· Parole Commission Actions
· Court Ordered Payments
· Work Release
· Inmate Control Status

Figure V-4

Statewide Magistrate System and Statewide Identification Index

The statewide Magistrate System, combined with the implementation of data standards, will eliminate much redundant data entry. In addition, the magistrate process will greatly benefit from increased data access to sentencing and criminal history information.

The Statewide Identification Index will add minor redundancy to the database. The index will contain the names and aliases of offenders along with a snapshot of current location, state and federal identification numbers, and other demographics. The Statewide Identification Index will reference a person's record throughout multiple databases. In addition, an application will allow a user to access summary information about each event. Introduction of data redundancy is acceptable because it allows users a tool to access information throughout the network. Figure V-5 shows this model.

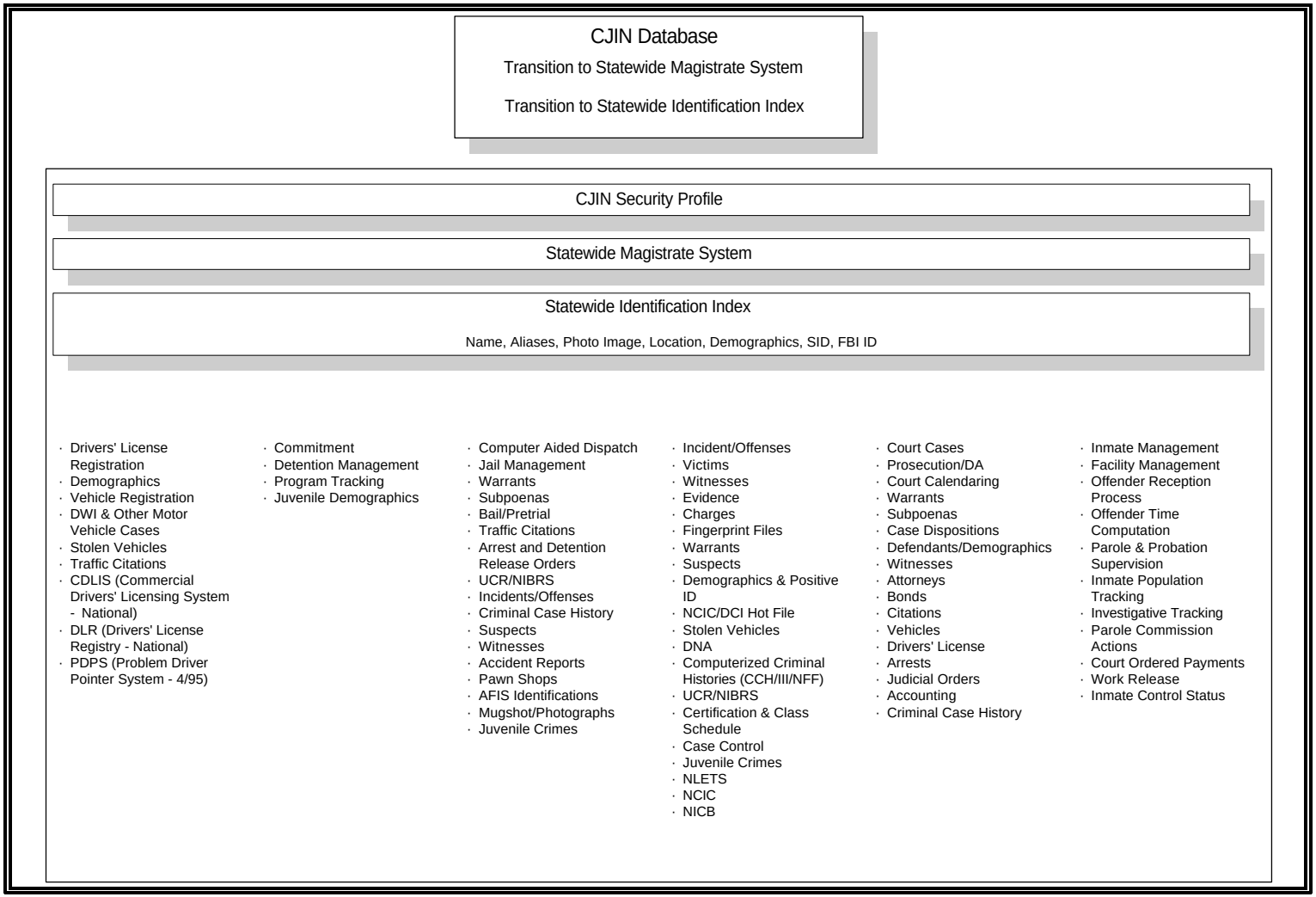

CJIN Database
Transition to Statewide Magistrate System
Transition to Statewide Identification Index
CJIN Security Profile
Statewide Magistrate System
Statewide Identification Index
Name, Aliases, Photo Image, Location, Demographics, SID, FBI ID
· Drivers' License Registration
· Demographics
· Vehicle Registration
· DWI & Other Motor Vehicle Cases
· Stolen Vehicles
· Traffic Citations
· CDLIS (Commercial Drivers' Licensing System - National)
· DLR (Drivers' License Registry - National)
· PDPS (Problem Driver Pointer System - 4/95)
· Commitment
· Detention Management
· Program Tracking
· Juvenile Demographics
· Computer Aided Dispatch
· Jail Management
· Warrants
· Subpoenas
· Bail/Pretrial
· Traffic Citations
· Arrest and Detention Release Orders
· UCR/NIBRS
· Incidents/Offenses
· Criminal Case History
· Suspects
· Witnesses
· Accident Reports
· Pawn Shops
· AFIS Identifications
· Mugshot/Photographs
· Juvenile Crimes
· Incident/Offenses
· Victims
· Witnesses
· Evidence
· Charges
· Fingerprint Files
· Warrants
· Suspects
· Demographics & Positive ID
· NCIC/DCI Hot File
· Stolen Vehicles
· DNA
· Computerized Criminal Histories (CCH/III/NFF)
· UCR/NIBRS
· Certification & Class Schedule
· Case Control
· Juvenile Crimes
· NLETS
· NCIC
· NICB
· Court Cases
· Prosecution/DA
· Court Calendaring
· Warrants
· Subpoenas
· Case Dispositions
· Defendants/Demographics
· Witnesses
· Attorneys
· Bonds
· Citations
· Vehicles
· Drivers' License
· Arrests
· Judicial Orders
· Accounting
· Criminal Case History
· Inmate Management
· Facility Management
· Offender Reception Process
· Offender Time Computation
· Parole & Probation Supervision
· Inmate Population Tracking
· Investigative Tracking
· Parole Commission Actions
· Court Ordered Payments
· Work Release
· Inmate Control Status

Figure V-5

Statewide Criminal History

This project will centralize and integrate the storage of criminal history information. Criminal history is one of the most redundantly stored data areas in the current model. The integrated history will implement further use of the SID number and cycle tracking number. Centralization of the criminal history information will migrate data from agency databases. This migration is depicted in Figure V-6 by the arrows from multiple agency databases to the central repository.

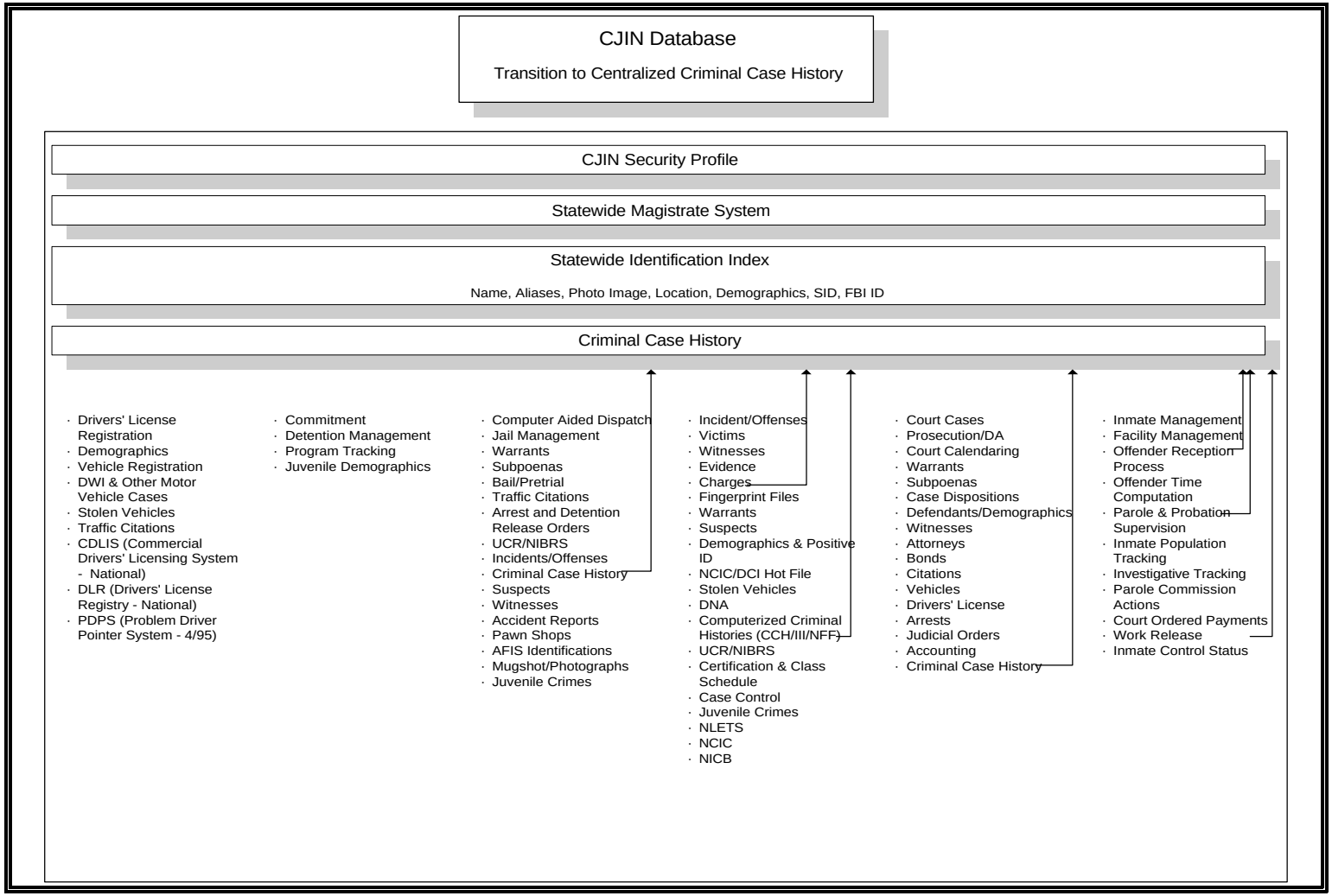

CJIN Database
Transition to Centralized Criminal Case History
CJIN Security Profile
Statewide Magistrate System
Statewide Identification Index
Name, Aliases, Photo Image, Location, Demographics, SID, FBI ID
Criminal Case History
· Drivers' License Registration
· Demographics
· Vehicle Registration
· DWI & Other Motor Vehicle Cases
· Stolen Vehicles
· Traffic Citations
· CDLIS (Commercial Drivers' Licensing System - National)
· DLR (Drivers' License Registry - National)
· PDPS (Problem Driver Pointer System - 4/95)
· Commitment
· Detention Management
· Program Tracking
· Juvenile Demographics
· Computer Aided Dispatch
· Jail Management
· Warrants
· Subpoenas
· Bail/Pretrial
· Traffic Citations
· Arrest and Detention Release Orders
· UCR/NIBRS
· Incidents/Offenses
· Criminal Case History
· Suspects
· Witnesses
· Accident Reports
· Pawn Shops
· AFIS Identifications
· Mugshot/Photographs
· Juvenile Crimes
· Incident/Offenses
· Victims
· Witnesses
· Evidence
· Charges
· Fingerprint Files
· Warrants
· Suspects
· Demographics & Positive ID
· NCIC/DCI Hot File
· Stolen Vehicles
· DNA
· Computerized Criminal Histories (CCH/III/NFF)
· UCR/NIBRS
· Certification & Class Schedule
· Case Control
· Juvenile Crimes
· NLETS
· NCIC
· NICB
· Court Cases
· Prosecution/DA
· Court Calendaring
· Warrants
· Subpoenas
· Case Dispositions
· Defendants/Demographics
· Witnesses
· Attorneys
· Bonds
· Citations
· Vehicles
· Drivers' License
· Arrests
· Judicial Orders
· Accounting
· Criminal Case History
· Inmate Management
· Facility Management
· Offender Reception Process
· Offender Time Computation
· Parole & Probation Supervision
· Inmate Population Tracking
· Investigative Tracking
· Parole Commission Actions
· Court Ordered Payments
· Work Release
· Inmate Control Status

Figure V-6

Statewide Warrant Repository

The warrant repository eliminates redundant entry and storage of warrant information. The arrows on Figure V-7 represent the migration of information from agency databases to a central repository. Movement of information to the repository will increase the accuracy, timeliness, and access to warrant information.

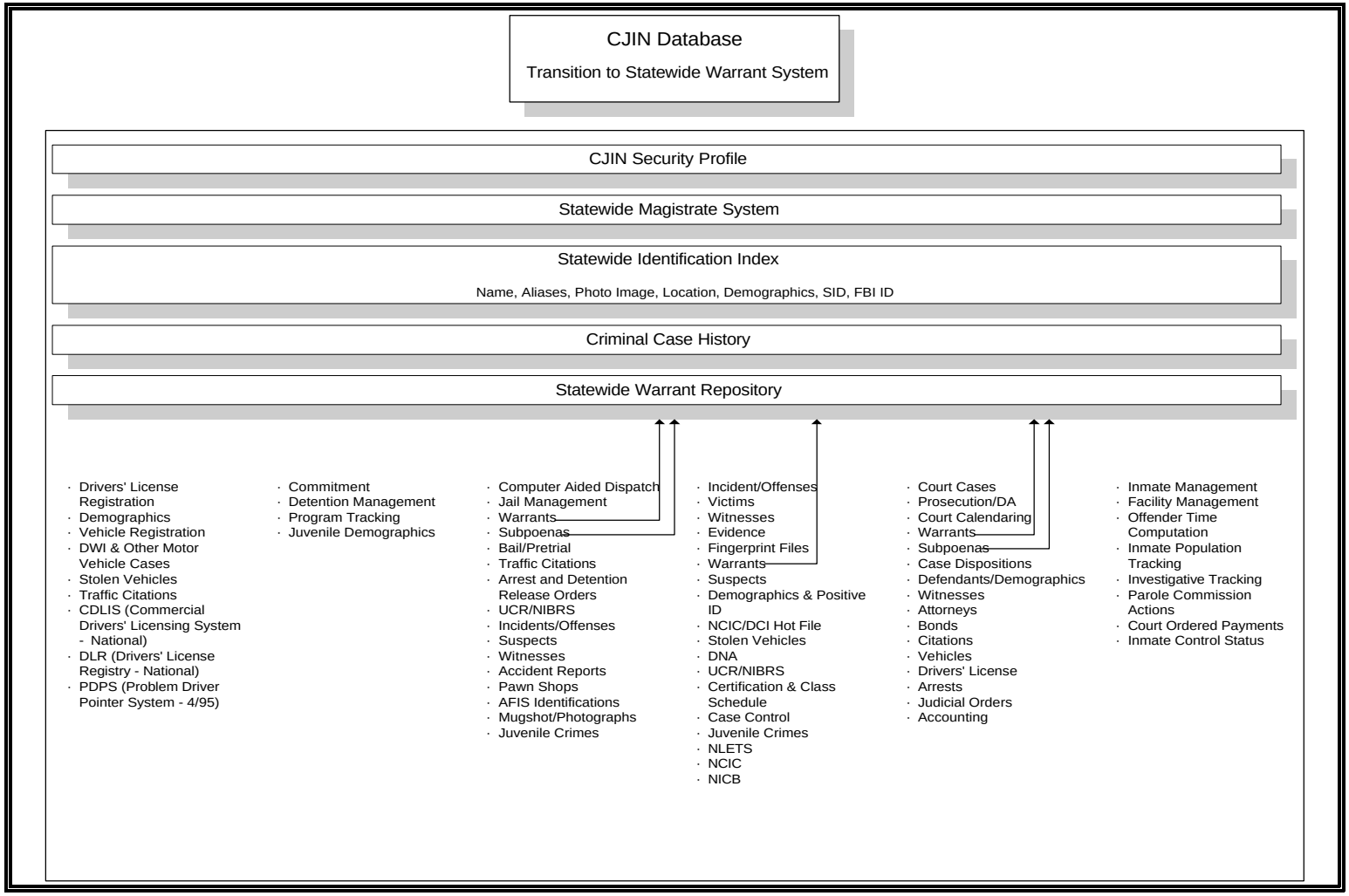

CJIN Database
Transition to Statewide Warrant System
CJIN Security Profile
Statewide Magistrate System
Statewide Identification Index
Name, Aliases, Photo Image, Location, Demographics, SID, FBI ID
Criminal Case History
Statewide Warrant Repository
· Drivers' License Registration
· Demographics
· Vehicle Registration
· DWI & Other Motor Vehicle Cases
· Stolen Vehicles
· Traffic Citations
· CDLIS (Commercial Drivers' Licensing System - National)
· DLR (Drivers' License Registry - National)
· PDPS (Problem Driver Pointer System - 4/95)
· Commitment
· Detention Management
· Program Tracking
· Juvenile Demographics
· Computer Aided Dispatch
· Jail Management
· Warrants
· Subpoenas
· Bail/Pretrial
· Traffic Citations
· Arrest and Detention Release Orders
· UCR/NIBRS
· Incidents/Offenses
· Suspects
· Witnesses
· Accident Reports
· Pawn Shops
· AFIS Identifications
· Mugshot/Photographs
· Juvenile Crimes
· Incident/Offenses
· Victims
· Witnesses
· Evidence
· Fingerprint Files
· Warrants
· Suspects
· Demographics & Positive ID
· NCIC/DCI Hot File
· Stolen Vehicles
· DNA
· UCR/NIBRS
· Certification & Class Schedule
· Case Control
· Juvenile Crimes
· NLETS
· NCIC
· NICB
· Court Cases
· Prosecution/DA
· Court Calendaring
· Warrants
· Subpoenas
· Case Dispositions
· Defendants/Demographics
· Witnesses
· Attorneys
· Bonds
· Citations
· Vehicles
· Drivers' License
· Arrests
· Judicial Orders
· Accounting
· Inmate Management
· Facility Management
· Offender Time Computation
· Inmate Population Tracking
· Investigative Tracking
· Parole Commission Actions
· Court Ordered Payments
· Inmate Control Status

Figure V-7

Juvenile Records Automation and Future CJIN Database

Figure V-8 represents the database changes that result from the implementation of the Juvenile Records Automation Project. Highlights of the changes include the addition and automation of juvenile court record tracking at the AOC, automation of the information tracked by the Department of Human Resources, Division of Youth Services, access to juvenile information from law enforcement personnel, and use of the Statewide Identification Index to access juvenile information. **All access to juvenile information in CJIN will continue to be strictly secured.**

Figure V-8 also represents data subject areas in the target CJIN database. The target diagram depicts non-redundant data subject areas distributed throughout the network. A summary index layer supports name and identification searches and contains the most recent location and demographic information.

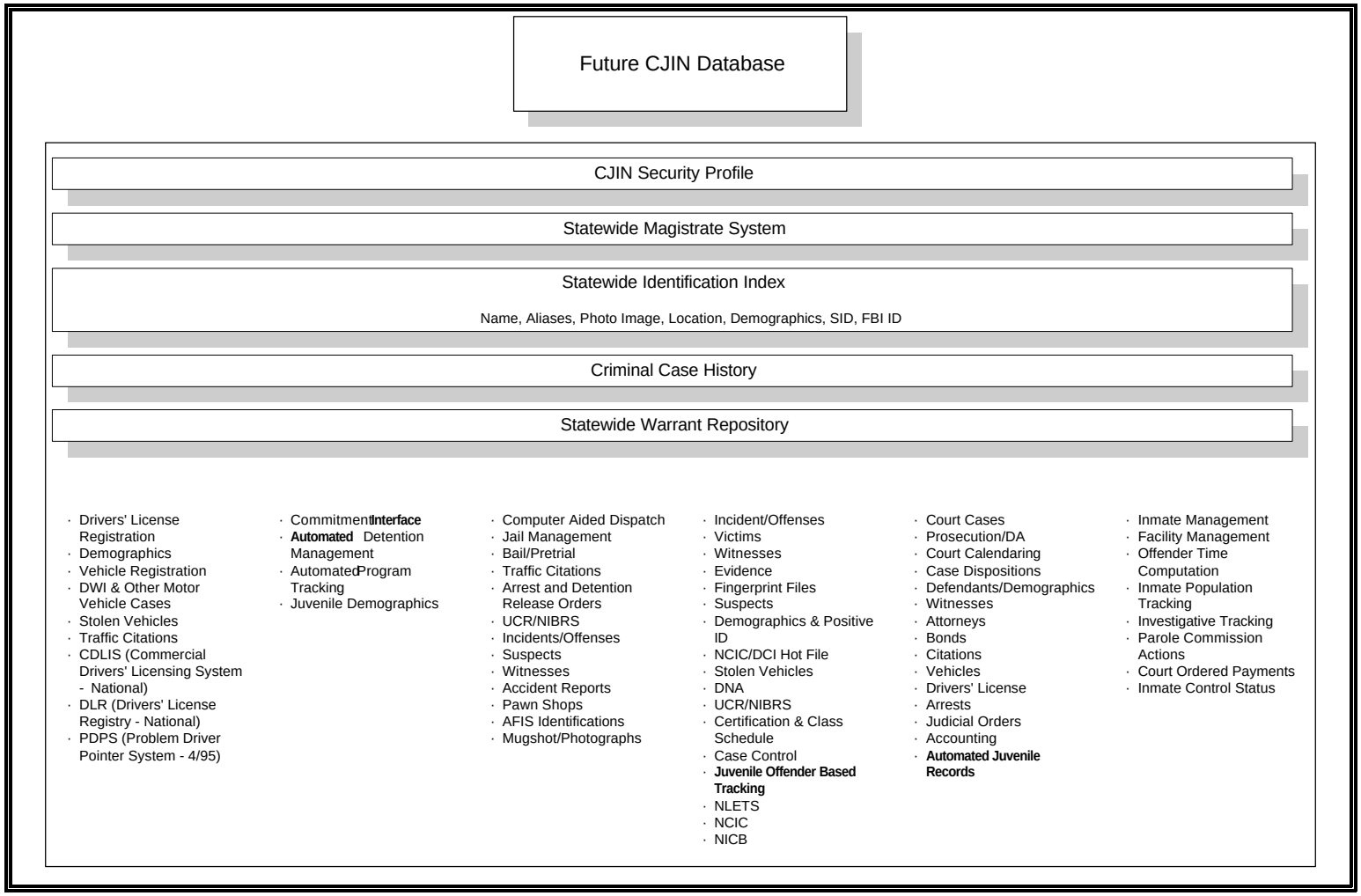

Future CJIN Database
CJIN Security Profile
Statewide Magistrate System
Statewide Identification Index
Name, Aliases, Photo Image, Location, Demographics, SID, FBI ID
Criminal Case History
Statewide Warrant Repository
· Drivers' License Registration
· Demographics
· Vehicle Registration
· DWI & Other Motor Vehicle Cases
· Stolen Vehicles
· Traffic Citations
· CDLIS (Commercial Drivers' Licensing System - National)
· DLR (Drivers' License Registry - National)
· PDPS (Problem Driver Pointer System - 4/95)
· Commitment Interface
· Automated Detention Management
· Automated Program Tracking
· Juvenile Demographics
· Computer Aided Dispatch
· Jail Management
· Bail/Pretrial
· Traffic Citations
· Arrest and Detention Release Orders
· UCR/NIBRS
· Incidents/Offenses
· Suspects
· Witnesses
· Accident Reports
· Pawn Shops
· AFIS Identifications
· Mugshot/Photographs
· Incident/Offenses
· Victims
· Witnesses
· Evidence
· Fingerprint Files
· Suspects
· Demographics & Positive ID
· NCIC/DCI Hot File
· Stolen Vehicles
· DNA
· UCR/NIBRS
· Certification & Class Schedule
· Case Control
· Juvenile Offender Based Tracking
· NLETS
· NCIC
· NICB
· Court Cases
· Prosecution/DA
· Court Calendaring
· Case Dispositions
· Defendants/Demographics
· Witnesses
· Attorneys
· Bonds
· Citations
· Vehicles
· Drivers' License
· Arrests
· Judicial Orders
· Accounting
· Automated Juvenile Records
· Inmate Management
· Facility Management
· Offender Time Computation
· Inmate Population Tracking
· Investigative Tracking
· Parole Commission Actions
· Court Ordered Payments
· Inmate Control Status

Figure V-8

The representation of a single database in the high level data model does not imply that all of the databases will be combined to create a centralized CJIN database. The model depicts the view of the database to a CJIN user. Through distributed database management and an enterprise gateway, the data will appear to the user as if it resides in a single CJIN database. The user will have access to criminal justice information despite its physical location in state or local databases.

Each organization's gateway will allow views of the data that are meaningful to satisfy the needs of its users. For example, an AOC user may query criminal case information and receive felonies and misdemeanors. However, a local law enforcement officer requesting the same history before approaching a suspect may receive only felonies.

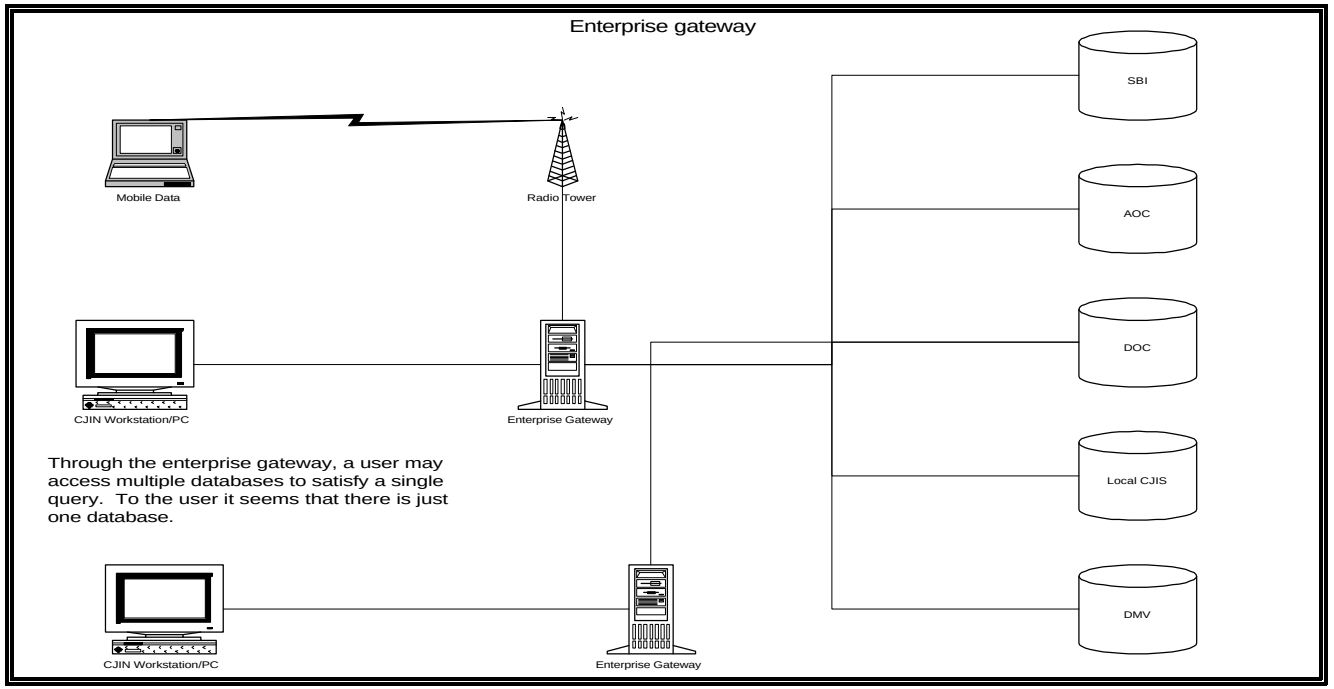


Figure V-9

Benefits of the Target Database

- Data definitions will be standardized. Standardization will lessen the expense of new system development and facilitate sharing information in the network environment.
- Data can be accessed by any authorized user despite its physical location.
- The new model eliminates redundancy and streamlines data management. This enhances the overall accuracy, reliability, and timeliness of criminal justice information.
- Enhanced event identification increases the assignment of dispositions to all charges.
- Enhanced use of the SID broadens the breadth and reliability of the criminal case history.
- Migration to a relational database management system in every agency promotes flexibility in meeting evolving state and federal needs.
- Relational database views and use of enterprise gateways allow agencies to structure queries, satisfying custom information needs.
- Data sharing eliminates redundant data entry, saving entry time and increasing the accuracy and timeliness of the data.

Constraints of the Target Database

- New technologies require significant retraining of support personnel.
- Organizations may be requested to relinquish autonomy over data elements that are currently redundant. These organizations may interpret standardization and data sharing as an encroachment on their authority.
- Existing databases may require reengineering to migrate to a relational, distributed database management system.
- Existing databases may require reengineering to implement standard codes, identifiers, and data structures.

CJIN Network Architecture

This section provides an overview of the envisioned target CJIN architecture which will support the diverse needs of the CJIN community. The target architecture is designed to facilitate communications from local to state organizations and communications among local agencies. This architecture is presented as the preferred solution which appears best suited to meet access and control requirements. Additionally, it is in compliance with IRMC standards and is consistent with current and planned investments.

Overview

The objective of the CJIN network architecture is to provide a path for interoperability between computer systems and applications which adheres to IRMC and industry standards. Adherence to the target architecture will simplify network planning, enable the construction of metropolitan area networks, facilitate the deployment of a distributed computing environment, and eventually minimize overall network cost. One example of how this strategy may be applied is when a local law enforcement system and a court system are located in the same vicinity. Instead of each agency having their own leased line back to Raleigh, they may share the same on ramp to the North Carolina Information Highway (NCIH) which through its network, will then relay the information to Raleigh or any other system in the network. With this type of topology, the shared use of a line reduces ongoing costs and the shared use of network connectivity devices, such as routers, reduces installation costs. A second advantage of this architecture is that information which is sent from a local

law enforcement system to a local courts system may not need to be routed through a central hub (Raleigh), which reduces network traffic and improves local performance.

Instrumental in the deployment of this network architecture is the NCIH. The NCIH has the potential to provide the network capacity necessary for envisioned imaging and text applications. It will provide the necessary high-speed links among mainframes and connectivity to local agencies through a variety of connectivity options. Additionally, it may provide video conferencing and interactive video solutions necessary for applications such as video arraignment. If used appropriately, it could provide a cost-effective solution to the accumulative network requirements imposed by CJIN.

CJIN network architecture is based on the following technologies:

- Transmission Control Protocol / Internet Protocol (TCP/IP) communications
- High speed local and wide-area connections based on NCIH and ANCHORNet networks
- Existing mainframe systems
- Server-based systems
- Intelligent end-user workstations
- Network-wide security

CJIN Network Strategy

The network will provide the CJIN user community with enhanced access to information. CJIN will support improvements in efficiency, productivity, and effectiveness. Initially the network will, to the greatest extent possible, utilize existing investments in mainframe technologies. Over time, these legacy systems will coexist with newer server-based applications, as they are developed.

Users will access the CJIN network using a variety of terminals and workstations. Information will be provided to the user's desktop in a consistent and usable format. Mobile users, especially law enforcement users, will benefit from the additional information that will be available through the network. Over time, all CJIN users will migrate to using intelligent workstations to access information over the network.

The CJIN network will provide the following benefits:

- High levels of network reliability and availability
- High-speed access to CJIN data
- Transparent access to information regardless of where it resides in the network
- Enhanced network security

Network Architecture

The CJIN network diagram (Figure V-10) defines a high level view of the CJIN network. The following CJIN computer systems are included in the diagram:

- AOC mainframe
- SIPS mainframe (DOC and DMV)
- SBI mainframe

These systems will be connected via a high speed wide-area network. CJIN will use TCP/IP, a suite of industry-standard communications protocols, to support the inter-system exchange of information. The CJIN network will be a private communications network. Existing and planned SIPS communications services will be used to define the network.

Local area network users will be connected to the CJIN network. These users will be able to access CJIN information directly without going through intermediary systems. Intelligent client workstations will request information from multiple computer databases. Information will be presented to the user in a concise and understandable form.

Existing terminal users will continue to access native departmental applications and databases through the mainframe. The CJIN network will allow these systems to exchange information directly. Specialized software agents will be able to poll the necessary databases for the necessary data. Information will be retrieved and presented to the terminal user as part of an integrated CJIN view.

Over time, new applications will be developed. Some of these may be client-server applications. These servers will be connected to the CJIN network. Mainframe and client-server applications will coexist on the network. CJIN users will be able to access information regardless of where it is located.

North Carolina CJIN
TCP/IP Network Architecture

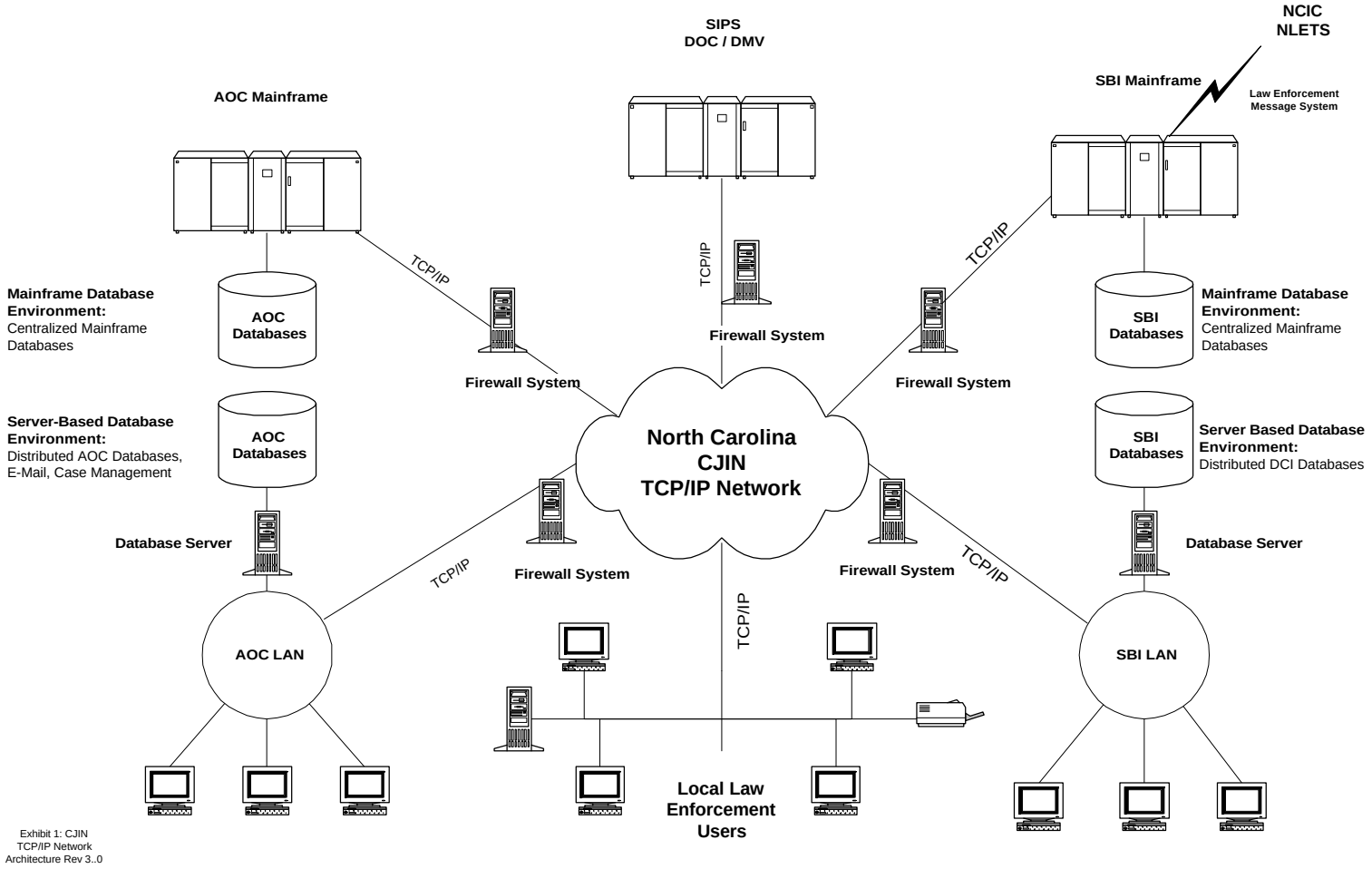


Figure V-10

Desktop Systems

CJIN desktop systems will include both intelligent workstations and terminal-based systems. Workstation computing systems will be assembled using commercial off-the-shelf (COTS) technologies. Advanced standards-based workstation computing will provide CJIN users with the following benefits:

- Modular, scalable computing systems
- Standardized desktop operating systems
- An industry standard graphical user interface
- Open computing model

Over time, existing terminals will be replaced with intelligent workstations which will enable applications to incorporate graphical images, voice, and video information. These data-intensive applications will require higher network throughput which will increase demands on the network.

Mobile Systems

Mobile computing systems will be deployed throughout the CJIN user community and are expected to become a standard law enforcement tool. It is expected that mobile units, including bar code readers, magnetic strip readers, and pen-based computers will have full access to the CJIN network.

Migration of Existing Criminal Justice Networks

The existing criminal justice networks will coexist with the CJIN network during the migration stage. Each CJIN agency will require a network review to determine the best approach to network integration. The migration strategies of all organizations involved will need to be closely coordinated to achieve cost reductions, improve service, and mitigate potential network performance problems.

CJIN Security

CJIN security components are those hardware and software modules that are required to fully address the authorization, authentication, access, and encryption of CJIN data. Existing criminal justice computer system and application security features will not be adequate in the future. The need to interconnect CJIN databases and allow access to authorized users via a CJIN network and the North Carolina Information Highway (NCIH) will require additional tools and methods to help protect CJIN information from unauthorized access. Additionally, CJIN connectivity to the Internet and other public networks will require specialized hardware and software to protect sensitive data.

Current System Security

The current security used by the various criminal justice agencies utilizes traditional system-based security. User accounts, logon IDs, and access profiles are used to grant or restrict access to the system, the applications, and the data. System access is generally restricted to workstations and personal computers directly connected to a local or wide-area network. Little or no end-user dial up access is supported on these systems. These private network systems provide adequate access control if standard security policies and procedures are implemented and enforced.

Future Security Requirements

Future CJIN security must provide effective protection for CJIN data in an open-network environment. Authorized CJIN users need to be able to access CJIN applications and data from anywhere within the CJIN network. Additionally, law enforcement mobile data terminals will become standard in patrol vehicles. CJIN security must provide the CJIN user community with unrestricted access to authorized data and applications.

As interagency computing becomes a standard part of the CJIN computing model, agencies will need to provide view-only as well as update access to existing applications and data. Users equipped with powerful desktop computers will, over time, come to expect and will demand unimpeded access to the CJIN information necessary to performing their assignments.

Future CJIN security will, when fully implemented, provide the necessary user access and network security. CJIN security will address the following:

- Authorization
- Authentication
- Encryption
- Public access

Authorization

CJIN user authorization will be validated using conventional password-based security. A user will be required to enter a user identification number, referencing a pre-established user account, and a password to gain access to a system or server. The user account and password will be verified before granting access to the system. The authorization step in CJIN security will be essentially the same as that of current system access controls.

Authentication

In addition to authorization security, CJIN will incorporate trusted third-party authentication. Trusted third-party authentication ensures that passwords are never transmitted as readable text across the network. In addition, the identity of the user cannot be tampered with en route to the ticket-granting service, and the application access tickets and privilege attribute certificates cannot be falsified. Third-party authentication can provide network-wide access with a single user logon. This will greatly simplify the administration of CJIN security. The Kerberos system, first developed at the Massachusetts Institute of Technology, is an example of a trusted third-party security system that uses a combination of public keys and private-keys to encrypt passwords and authorization codes. The following diagram (Figure V-11) provides an overview of the Kerberos process.

Kerberos Security Services

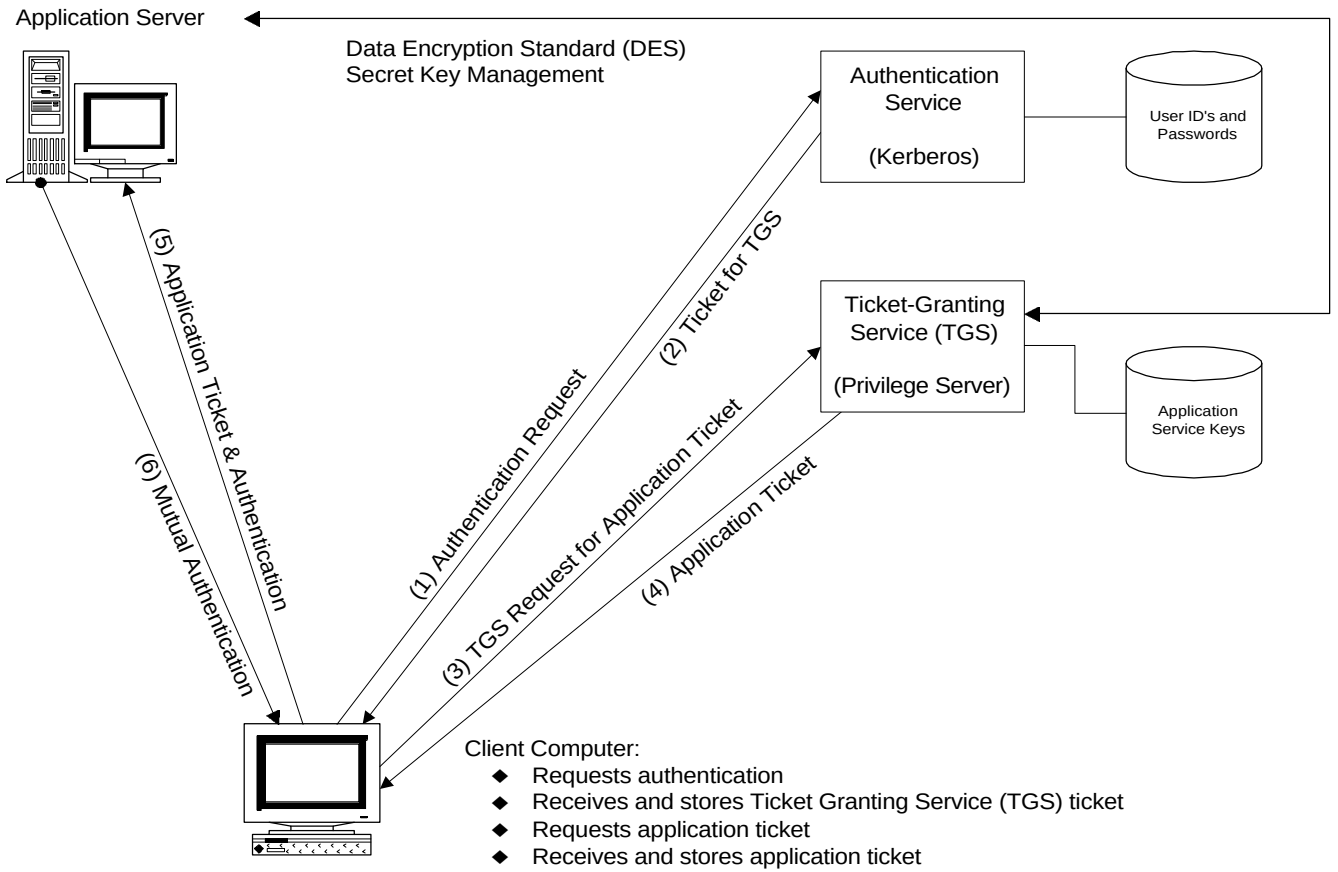


Figure V-11

The use of public key / private key authentication as a CJIN security measure will have the following limitations:

- The CJIN user workstation must be able to locally execute a logon program as well as store and forward the resulting tickets and certificates

  Mainframe terminals will not be able to execute a logon program. Custom mainframe software may have to be written to provide terminal support for authentication.

- Existing CJIN applications will have to be modified to accept the resulting tickets

  This will require a significant amount of time and effort due to the large number of CJIN systems and applications that must be modified.

- Authentication message traffic will impact the overall CJIN network

  Minimizing this will require the use of time windows during which the workstation can dynamically generate new authentication codes without requiring access to the trusted service.

Encryption

CJIN will require encryption of passwords, keys, and data. Both single key and double-key encryption will be used. Single-key encryption, as embodied in the National Institute of Standards and Technology (NIST) Data Encryption Standard (DES), will be used for inter-process communications between servers. In addition, over-the-air transmission of CJIN mobile data will be encrypted using DES.

Double-key encryption technology, originally developed at both Stanford University and MIT, is available commercially from RSA Data Security, Incorporated and other vendors. Double-key encryption allows for secure transmission of data

over a public network. This type of encryption is also known as public key private key encryption. The CJIN trusted third-party authentication process previously described will use public key private key encryption. This security strategy can provide for electronic signature verification of transmitted information.

Public Access

Public access, in this context, refers to the connection of the CJIN network, a private network, to other outside networks. Examples of these are the NCIH and the Internet. Connection of CJIN to any public (non-CJIN) network will require special network security precautions. Firewalls, specialized software programs that reside in routers and dedicated servers, will guard against unauthorized access to the CJIN network.

Commercial firewall software products are readily available. Firewall technology, while not new, has recently become a critical network component as more organizations are required to connect their systems and networks to outside users. Firewall technology will continue to evolve as computer hackers develop new means of bypassing network security. CJIN firewall security will be an additional network expense. In addition, firewalls may degrade CJIN network performance and throughput. To be effective, firewall systems may have to be installed in every instance where a CJIN system connects to an outside network. The firewall system will be an additional link in the connection between a user and the requested application or data. This additional link, and the associated overhead, may degrade overall performance.

Applicable Standards

The following standards will be addressed by a CJIN-wide security system:

- Distributed Computing Environment (DCE) security
- Data Encryption Standard (DES)
- Kerberos authentication
- RSA security
- Firewall security

Technical Constraints

Success of CJIN is dependent upon recognizing and managing those constraints that directly impact the implementation of CJIN technologies. In addition, standards are still evolving that will directly impact the state's ability to implement CJIN technology-based solutions.

Those technology constraints that will impact CJIN include:

- High speed wide-area communications
- Network security
- Data compression

High-Speed Communications

The State will require a high speed wide-area communications network that is capable of supporting the high volume of CJIN data traffic. General State Information Processing Services (SIPS) communications offerings currently available are of a limited bandwidth. North Carolina Information Highway (NCIH) communications, while offering higher speed communications, are currently constrained by limited options for allocating high speed multi-megabit links. Vendor enhancements to current ATM offerings will enable the state to make efficient use of these high-speed links. Switched Virtual Circuits (SVCs), a service that will be required before ATM can be of practical use with CJIN, is not currently available. Permanent Virtual Connections (PVCs), a non-real-time method of managing virtual connections, are currently the only available option.

Network Security

Proven network security will be required by CJIN before users are granted access to systems, applications, and data. Firewall technologies may degrade overall CJIN performance and throughput. Commercial firewall products will continue to evolve. Firewall security is currently a technology area with few defined standards. Until industry standard

products can be developed, and the technology matures, the need for CJIN security will require implementation of closed-architecture firewall solutions.

CJIN security will require that effective access control and user authentication techniques are implemented. Proposed standards for a distributed computing environment (DCE) include optional security modules. CJIN application security will require implementing DCE Kerberos or other suitable methods of user authentication. Current CJIN departmental applications were not designed to support distributed computing. These applications will require modification before end-user workstation applications can access CJIN data.

Data Compression

Current NCIC standards for electronic fingerprint files do not provide for file compression. Until recently, the available grey-scale image compression methods altered and degraded the fingerprint image. Recently developed compression techniques provide for up to a 15-times reduction in the size of the fingerprint image file while maintaining acceptable fingerprint image quality. These new data compression methods are not yet approved for NCIC transmissions. NCIC fingerprint files are a major factor in defining CJIN network bandwidth requirements and capacity planning. Close coordination with NCIC requirements and standards will be required to properly size the CJIN wide-area network. It is estimated that data compression of NCIC fingerprint images will reduce the related network load on the CJIN network by one order of magnitude.

Emerging Technology Standards

The following technology standards will impact CJIN:

- **NCIC 2000**

  NCIC 2000 standards will significantly impact CJIN technologies. Network infrastructure, communications protocols, and end-user workstations will be impacted by the new NCIC standards. Of primary significance will be the transmission of electronic fingerprint image files. The state will require a high-speed network capable of handling the high volume of data traffic that will be generated by CJIN electronic fingerprint files. The volume of

fingerprint data traffic will be compounded by the need to fingerprint all misdemeanants. Data compression, when approved for fingerprint files by NCIC, may reduce the overall network load.

NCIC 2000 standards will require intelligent PC-based workstations. The original NCIC-defined workstation specification, a 80386-based PC with 4 MB RAM memory, has been upgraded to a 80486 DX2-66 processor with 8 MB of RAM memory. Even as the State begins to deploy NCIC-compliant workstations, because NCIC workstation requirements may continue to increase, the minimum workstation configuration may continue to change. This will entail additional expenditures to upgrade existing workstations.

- **APCO 25**

APCO 25 (Associated Public-Safety Communications Officers) standards for public safety radio are expected to be completed and published by the summer of 1995. It is expected that vendors will require 18 months to deliver APCO 25 compliant radio equipment. Existing 800 MHz radios will require field upgrades or wholesale replacement to be APCO 25 compatible. Although APCO 25 is an industry standard, not all vendors have embraced the standard. State and local procurements that specifically require APCO 25 compliant radio equipment may be constrained by protracted procurement litigation.

- **ATM Switched Virtual Circuits**

The broadband signaling standards required to support high speed switching are not yet complete. Until such standards are implemented, the Fujitsu model FEDEX-150 ATM switches, currently in use within the state as part of the NCIH and SIPS network, are only capable of non-real-time switched virtual circuits (SVCs). Real-time SVC service will be required before CJIN can be implemented over a wide area at a high (45 MBit/sec) speed. Until the necessary signaling standards are defined and implemented, CJIN traffic will be limited to using SMDS at a DS1 speed of 1.5 MBit/sec.

CJIN Project Strategy

The following section provides a detailed discussion of the strategic projects that have been recommended as supporting the objective and goals for development of the Criminal Justice Information Network. Each project has been chosen for its overall impact on the advancement of CJIN as a whole. Projects are not included that address the needs of a specific agency, but are not of critical strategic importance to the CJIN enterprise.

Each project includes a review of the current situation, an examination of the need for change, and a detailed explanation of the recommended solution. A summary page precedes each project and is designed to provide the reader with a quick review of the pertinent points.

The recommended projects fall into three implementation categories:

- ***CJIN Management Structure Development***

These projects support the process of building the organizational structure to support the long-term development of CJIN.

- ***CJIN Infrastructure Development Strategy***

These projects support the process of building the technical infrastructure to support the long-term development of CJIN.

- ***CJIN Applications Development Strategy***

These projects are developed within the CJIN infrastructure and their purpose is to address the most critical, strategic information needs as they apply to the Criminal Justice Information Network.

Our project implementation strategy is presented in Figure VI-1. A discussion of the recommended approach and priority of implementation within each of these categories is presented in this overview. The logical progression of projects and inter-dependencies has been considered in the approach, timing, and order of implementation.

CJIN Strategy

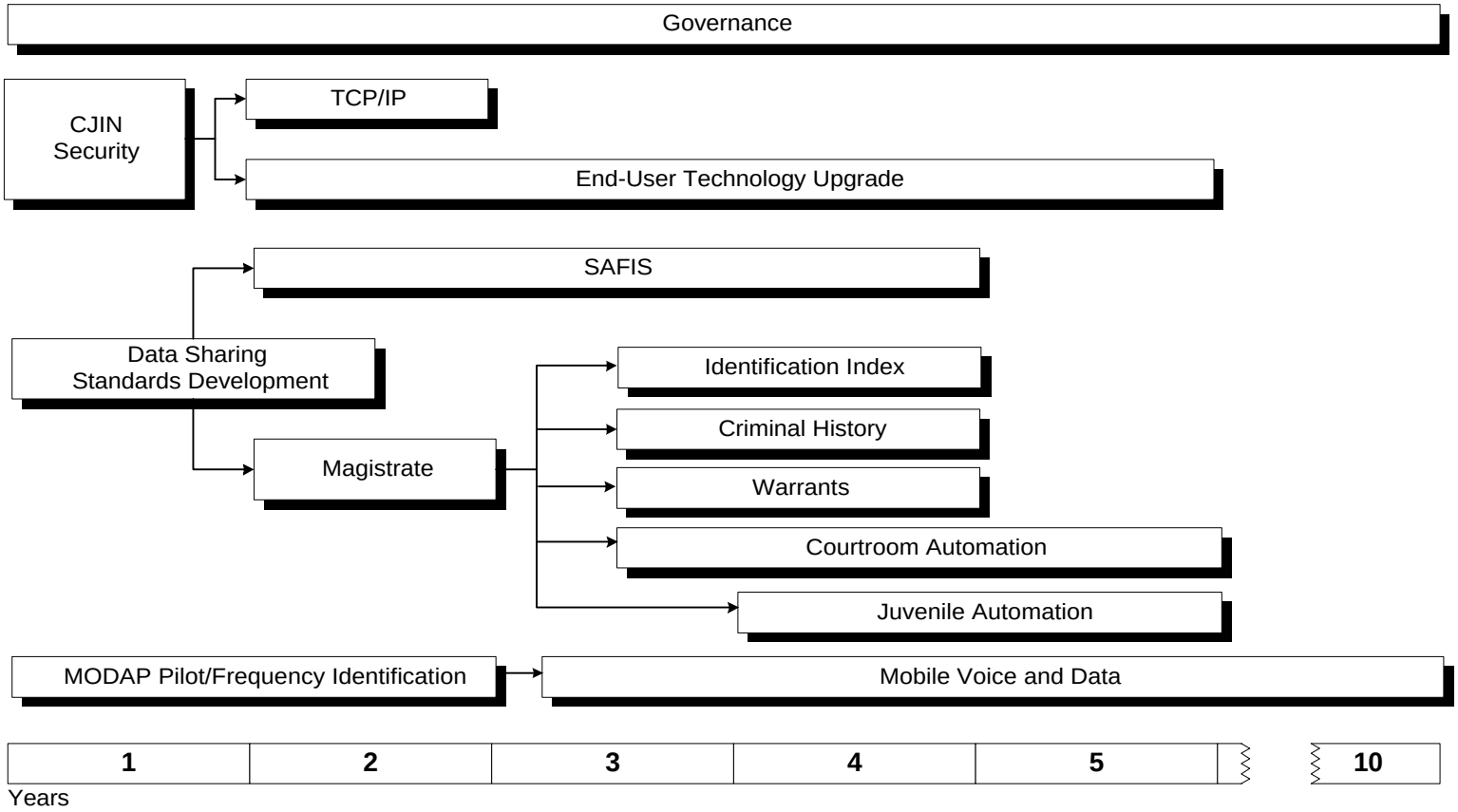


Figure VI-1

CJIN Management

Recommendation	*Description*
CJIN Governance	The critical first step in defining and implementing the CJIN infrastructure is creation of the CJIN Governance Board, as recommended in Section IV of this report. Strategic leadership from both the state and local levels is required to ensure the implementation of strategies and specific projects necessary to meet the CJIN objective and to realize the benefits of inter-operability related to long-term planning.

CJIN Infrastructure Projects

Recommendation	*Description*
1. Data Sharing Standards Development	This project should be initiated concurrent with or immediately after establishment of the CJIN Governance Board. Initially, a data sharing committee comprised of the data administrators from key state and local criminal justice agencies should begin the process of data dictionary definition, as this task may take 12 to 18 months. This group would eventually become a standing sub-committee to the CJIN Governance Board.
2. CJIN Security	Security measures must be implemented to protect sensitive information prior to connecting CJIN to public networks. This project will set the standard for data security and build in-house experience in deploying data security systems.

Recommendation	*Description*
3. TCP/IP	Implementation of TCP/IP communication protocols and services on all CJIN host systems will provide the communications structure to freely and uniformly exchange information necessary to support CJIN operations.
4. End-User Technology Upgrade	Phased installation of intelligent workstations is necessary to support CJIN connectivity, National Crime Information Center (NCIC) standards, CJIN security, and future CJIN applications.
5. Statewide Mobile Voice and Data	The procurement and implementation of both the mobile voice and data infrastructure and in-car units is not currently dependent on other CJIN projects in its initial phases. As the connectivity between systems increases and the reliability and accessibility of warrants and criminal history improves, the mobile user will require easy and timely access to this information.

CJIN Applications Projects

Recommendation	*Description*
6. Statewide Automated Fingerprint Identification System	Improvement in both the process and speed of subject identification is a key reason to implement the State Identification Number (SID) as the standard statewide identifier. Livescan digitized fingerprinting systems should be deployed at centralized counting booking intake centers and connected to the SBI / DCI statewide Automated Fingerprint Identification System (AFIS). The goal is to reduce the average time for positive subject identification by fingerprints from more than two weeks to less than two hours.
7. Statewide Magistrate System	A Statewide Magistrate System to automate the magistrate warrant creation and charging process should be implemented in all counties that are not automated. This project will provide a reduction in re-entry of case information, overall improvement in accuracy of information, and real-time availability of case information.
8. Statewide Identification Index	Implementation of a Statewide Identification Index (sometimes referred to as a master name index) built on the SID will provide the CJIN user an easy and effective method to link together offender information across multiple state and local databases and systems.
9. Statewide Criminal History Repository	All arrested misdemeanants should be fingerprinted and included in the SBI / DCI Criminal History Repository. Current statutes appear to allow this process. The implementation of livescan devices and the link to the SBI / DCI AFIS system will ease the increased workload of fingerprinting misdemeanants. We recommend that access to the Criminal History Repository be provided through the Statewide Identification Index.

Recommendation	*Description*
10. Statewide Warrant Repository	The implementation of the Statewide Magistrate System will provide the process to update the SBI / DCI statewide warrant repository on a near real-time basis with new and served warrant information. We recommend the creation of a physical warrant repository in the short term for each city / county and a long-term move to a "paper on demand" active warrant system.
11. Courtroom Automation	The courtroom is a critical point in the process where automation can significantly reduce redundant data entry, streamline the timeliness of information to the user, and prevent offenders from "slipping through the cracks" of the criminal justice system. Courtroom automation consists of real-time data input in the courtroom, automatic forms generation, automatic queues to next process, and automatic updates to case and criminal history.
12. Juvenile Records Automation	The AOC juvenile records and the Department of Human Resources (DHR) Division of Youth Services' (DYS) records should be automated. This effort should establish compatibility between the adult and juvenile CJIN components with anticipation of increased information sharing between these agencies in the future.

Project Costing

Each project described in this section includes an estimate of initial implementation and ongoing support costs. The estimated costs presented in this report are the blending of the following cost estimates:

- **Vendor Cost Estimates**

A variety of vendors that supply hardware, databases and criminal justice applications were contacted and asked to provided estimated costs for their respective products. We used vendors that either already have products installed in the state or provide products that are being considered for implementation by one or more agencies within the state.

- **Out of State Agency Cost Estimates**

As a result of our national best practices survey, we identified a number of states who had implemented projects that were similar to one or more of the projects we have recommended. We discussed with these agencies their estimates of person time for implementation and support of these efforts in their states.

- **North Carolina Agency Cost Estimates**

We spoke with both local and state agencies regarding their experience and costs in implementing past systems and their estimates to implement future systems that related to our recommended projects.

Costing Assumptions

Labor (project management, business process analysis, programming, training, etc.) has been calculated using a full-time equivalent (FTE) monthly cost of $22,000. This rate is equal to 160 hours per month at $137.50 per hour. The hourly rate is comprised of $120.00 for services and $17.50 for estimated travel expenses. It is expected that labor for these projects will be staffed by both state and local government employees as well as outside consultants. The estimated hourly rate assumes that the majority of services will be provided by outside consultants, due to current state and local

staffing constraints. The estimated hourly rate is used to provide a blending of the various labor and expense costs for analysis, design, programming and training.

All costs have been estimated in 1995 dollars.

DATA SHARING STANDARDS DEVELOPMENT

CURRENT SITUATION

- Data standards exist within each agency, but are not unified across agencies.

NEED FOR CHANGE

- States with plans for highly integrated criminal justice systems are developing statewide data dictionaries.
- Information is difficult to share between computer systems because there is a lack of a comprehensive cycle tracking number, common offense codes, common application program interfaces, and database views.
- There are disparate user security profiles across criminal justice information systems.
- Migration to a new technical architecture creates an opportunity for standardization of data.

RECOMMENDED SOLUTION

- Form a subcommittee of the CJIN governing body consisting of representatives from local and state criminal justice agencies.
- Develop, adopt, and enforce a statewide data dictionary including:
  1. Documentation of all common data definitions
  2. A comprehensive cycle tracking number
  3. Common offense code identifiers
  4. Application programming interfaces and common database views
  5. A statewide user security profile
- Perform data accuracy and completeness audits.

Current Situation

Data standards exist within each agency, but are not unified across agencies.

Agencies that will comprise CJIN developed information systems to meet their critical operating needs. These systems grew within single agencies, independent of one another. They are, therefore, based on different sets of standards. The Data Management Section of this report explains the need for the definition of statewide data standards. These standards are essential to facilitate data sharing between CJIN agencies.

Need for Change

States with plans for highly integrated criminal justice systems are developing statewide data dictionaries.

The national survey examined justice information integration in other states. The findings of the survey show those states with existing or planned integration of criminal justice information systems developed, or are developing, a statewide data dictionary. The extent of states' dictionaries varies, but each attempts at least to define common data elements. The state of Florida developed a good example. Florida's Offender Based Tracking System project (OBTS) resulted in the State Criminal Justice Data Element Dictionary, which was eventually adopted by North Carolina's Department of Correction for the development of their Offender Population Unified System (OPUS). Florida's efforts resulted in a Local Criminal Justice Data Element Dictionary as well.

Lack of a comprehensive cycle tracking number.

Of utmost importance to Florida's OBTS project was the limitation of scope to the elements necessary to track a defendant's cycle of events from inception to disposition. The term event is used to include arrest, booking, fingerprinting, adjudication, and many others in the justice process. The key element Florida standardized was an offender-based tracking number or OBTS number. This key is what we refer to in CJIN as a cycle tracking number.

The State Bureau of Investigation, Division of Criminal Investigation (SBI / DCI) tracks events by a check digit number. This unique number links information related to a single event. Law enforcement agencies assign a check digit number at fingerprinting. However, a number to track events for individuals who have not been fingerprinted does not exist. Lack of a unique key for all events inhibits tracking across the separate justice databases. Using the check digit number, Administrative Office of the Courts (AOC) and SBI / DCI have matched 90 to 95 percent of the felony arrest records with proper dispositions. Linking dispositions to non-fingerprint-based events has not been successful.

Offense codes vary between agencies.

The codes used to record charges are different across computer systems for two reasons. First, local law enforcement agencies require the capture of information at a greater level of detail than provided for by National Crime Information Center (NCIC) and Uniform Crime Reporting (UCR) summary reporting standards. Second, state and local systems evolved independently upon the basis of different charge identifiers. In other words, systems grew up speaking different languages.

Disparate charge identifiers pose a problem to CJIN. Lack of common codes makes passing of event charges difficult. The processes of adding, modifying, and disposing of charges often span multiple computer systems. The interfaces require translation of charge codes from one system to another. In order for a computer system to send charge information, it must maintain a cross reference table to the charge codes for every other system. These cross reference tables are difficult to maintain as statute or identifier changes must be made to every automated system.

Lack of common application program interfaces or database views.

Interfacing current databases is difficult because of a lack of standardized application program interfaces or database views. Application program interfaces define and publish data elements and business rules necessary to perform a transaction. Database views use relational database technology to allow an external user to view or add data. Agencies currently handle communication between systems on a case by case basis, identifying and mapping data elements. Each agency spends great amounts of time developing single interfaces rather than global definitions that can be reused.

Disparate user security profiles.

Each agency maintains profiles for users authorized to access their systems. Nevertheless, these profiles retain different types of information. With different security and profile data needs, organizations cannot assign access levels or authorize individuals to access data through the network.

Migration to a new technical architecture creates an opportunity for standardization of data.

Implementing technology will provide agencies the ability to share and access data more efficiently. However, without developing standards for the information, new efficiencies cannot be maximized. Increasing the connectivity between previously autonomous systems creates a need to consolidate the definition of the shared information. The full potential of new technology can be realized when coordinated with the opportunity to standardize information sources.

Recommended Solutions

Form a subcommittee of the CJIN governing board comprised of representatives from local and state criminal justice agencies for data sharing standards development.

The state of Florida's OBTS project was initiated by the adoption of a statutory amendment mandating charge dispositions to be reported by the Clerk of Courts rather than law enforcement agencies. The statute change initiated the formation of an interagency group with members from law enforcement, courts, and corrections. The committee coordinated the dictionary development, review, and adoption.

The development of a statewide data dictionary is a multifaceted process for North Carolina. The State must form a committee with representation from each CJIN agency including the Administrative Office of the Courts, Department of Transportation, Department of Correction, State Bureau of Investigation's Division of Criminal Information, State Highway Patrol, and local law enforcement. The committee should be a subcommittee to the CJIN governing board. The subcommittee will be responsible for developing, documenting, facilitating user approval, and implementing the data

dictionary. After the implementation of the dictionary, the subcommittee will also develop and conduct the data quality assurance audits.

In developing standards for the data elements, the committee must employ input from all concerned agencies. Data standardization should follow a phased approach, following information through the criminal justice process from an incident through post sentencing, including probation and correction. For adoption of the standards, participants in each phase must not only feel included, they must have confidence in the dictionary, and they must recognize and understand the benefits that their organization will receive. The state of Rhode Island expended the money and effort to develop a dictionary, but an unsuccessful implementation of the standards detracted significantly from its value.

Develop, adopt, and enforce a statewide data dictionary including:

1. Definition of all common data definitions.

The purpose of the data dictionary is to standardize, document, and publish enterprise metadata. Metadata is data about an organization's data. The Data Management section of this report describes the detail necessary in documenting metadata. The development of the dictionary will raise consolidation issues between organizations and develop a roadmap not only for the improvement of current interfacing, but for the development of the CJIN. Documentation of data location, all names and aliases by which the element is referred, and definition is essential to implementation of the distributed, relational database environment that will act as a foundation for CJIN.

2. A comprehensive cycle tracking number.

To assure the recording of disposition information for all events or episodes, the committee should develop a cycle tracking number that is not dependent upon the fingerprint process. CJIN should establish a unique identification number for events

including arrests, citations, warrants, court cases, and incarcerations. This number should link these events with or without inclusion of a fingerprint activity.

The cycle tracking number, linking the record as it progresses through the CJIN, will increase arrest records and charges being associated with proper dispositions. In addition, events linked by common identifiers across systems are easy to interface automatically. Development of disposition tracking based on a common identifier can eliminate redundant entry of information in the short term and dual entry of the event in the long term. In both the short and long term, implementation of the cycle tracking number greatly improves the accuracy, reliability, and timeliness of the criminal case history by increasing efficiency of the matching mechanism and broadening the number to include non-fingerprinted arrests.

3. Common offense code identifiers.

Definitions of common offense code identifiers must meet multiple requirements. They must meet requirements for federal NCIC and UCR reporting, state tracking, and local law enforcement. In arriving at common codes, the standards committee must balance all these requirements. One path is local modification of the NCIC charge codes centrally maintained in a CJIN reference table. Local modification adds increased information to federal standard reporting. However, it is important that the dictionary define the structure of charge code modifiers. Central maintenance reduces the overhead associated with changing a charge code in multiple computer systems.

Adoption of standard offense codes is a sensitive issue between state agencies and local authorities. Local law enforcement agencies feel that they give up quality of information in the name of standardization. The benefits of common codes must be clearly displayed to local authorities. These benefits include easier automation of passing charges between systems, elimination of maintenance of redundant charge translation tables, and more accurate and useable information populating the criminal history. Examples of better information include statistical reporting on criminal history, providing executive information to local authorities, easier and quicker tracking of dispositions, and a common base table allowing local agencies to track the processing of every charge on every arrest. Reporting will allow agencies to recognize officers not for making arrests, but for making arrests that result in convictions.

4. Application programming interfaces (API) and common database views.

In defining and publishing common data definitions, agencies can build interfaces upon a common data structure. Negotiation to map fields will occur in the development of standards, applying the overhead to many interface and interconnection projects over the life of CJIN. For example, organizations can build application programming interfaces, or APIs, which document data formats and rules for creating, updating, or deleting data. Developing common views and API's is an investment in overhead application that will benefit every interface between CJIN participants. In creating a network, development and documentation of common data elements is essential.

5. A statewide user security profile.

The data dictionary should define the requirement to be included in a common security profile. The elements included must meet current security requirements of state and local databases and the new requirements inherent in the network as well. The CJIN Network Security Project provides an analysis of security implementation. Definition and implementation of the profile will allow for uniform application of security across the network to make the users' view of one database possible.

Perform data accuracy and completeness audit.

A standardized data dictionary is quality *insurance*. Once the committee develops the dictionary, the audit is quality *assurance*. The audit will not only provide assurance of the accuracy and completeness of the data. It can be used to measure effectiveness of processes, timeliness of disposition entry, and compliance of local agencies to reporting requirements. The criminal history is developing into a tool for more than investigation. The history is being employed in background checks for public and private institutions, to make arrest decisions at the point of incident, and as a basis for structured sentencing. As CJIN becomes more accessible to state and local users throughout North Carolina, confidence in the database content is paramount. More agencies, inside and outside the criminal justice community, will base decisions upon the history information, pushing the need for a formal audit program to assure data quality, accuracy, and timeliness.

After developing and implementing data standards, the committee should validate the process through a series of data accuracy and completeness audits. The first of these audits will be the Criminal History Accuracy and Completeness Audit. This audit will consist of three phases, each verifying the criminal history information. First, the audit will check the data population records at the state and local level. It will then compare input documents with the CCH records using random sampling. Auditors will then perform statistical analysis of record completeness including, but not limited to, the percentage of disposed arrests.

Barriers and Risks

The benefits of a statewide data dictionary and a quality assurance audit program are numerous. However, the project is not without barriers. These barriers include:

Problems reaching standards agreement within the CJIN enterprise

Difficulty in reaching agreement is the most obvious risk. Possible complications include alienation of people or agencies in the standardization process and disagreement on the basis by which data should be tracked. Although the development team should contain representatives of some counties, there is a risk of alienating local agencies through mandated adoption of the statewide data dictionary. It is important to mitigate this risk by proving the benefits of increased data sharing. Smaller or less automated counties will cooperate with the development process if the dictionary can reduce or eliminate the costs of automation. Florida was able to reduce this risk in small and large counties by spreading the base of input and promising a prototype system to those without automation.

Different tracking basis

Another problem in reaching standards agreement may stem from the different way that law enforcement and the courts view data. Law enforcement agencies tend to base information on a particular defendant. The courts, on the other hand, are primarily case-based. Implementation of a statewide identifier and a cycle tracking number will reduce the conflict by allowing each group to track the data in a way that supports its needs. Law enforcement and prosecutors may track by defendant while the courts track by case.

Resistance to standards adoption

Local systems, especially larger, expensive systems, may resist adopting statewide standards. The cost in implementing the standards to some localities may be extensive. The AOC and Mecklenburg County have experience translating data from one system to the other. The burden to local criminal justice information systems cannot be overlooked. To reduce this barrier, the automated counties must have significant input into the standardization process. Counties must not feel that the state develops and mandates standards. They must believe that the state and the counties cooperate in developing the dictionary, which will be useful to statewide criminal justice without damaging local criminal justice.

Conversion of existing data to standard format

Adoption of data standards will be a migratory process. As state and local agencies develop new systems and reengineer systems for relational technology, standards can be adopted. But some standards, such as common offense codes, will need to be implemented in current systems. Legacy databases and the application programs that update these databases will need to be modified. Budgeting funds for the adjustments to current systems is important to the success of the standardization effort.

Noncompliance with the standards

Noncompliance is a later risk. After adoption, a county can misuse or misapply a standard. The state can best mitigate this risk through adherence to reporting requirements and application of the audit process. A standard is only as strong as its application within systems.

Resistance to audit

Localities must remain active participants in the audit process to eliminate resistance. There is a risk that some local organizations may oppose data quality checks if they are viewed as a state mandate. However, if local systems personnel are included in the process, they will not only augment data sharing with exposure to other systems, they will drive the audit process.

The data standardization is not without risks. Benefits to the CJIN community outweigh these risks. To mitigate risk and promote benefits, the standardization committee must employ local agencies as a large, if not the largest, contributor to the development of the dictionary and audit procedures. The largest risk is local resistance, but if the guidelines come from throughout the state this resistance can be minimized. The CJIN community must believe that standards have been cooperatively developed, not dictated by a detached authority.

Benefits

In addition to benefits unique to the cycle tracking number, common offense code identifiers, APIs, and standard security profiles, the following benefits are results of data standards and quality audits:

- Elimination of data entry and storage redundancy
- Higher data quality, reliability, and timeliness
- Increased completeness and accuracy of criminal history information
- Template base for use in new systems development at the state and local levels

- Better decisions based on better information at all levels of the criminal justice process
- Augmented processes for data capture and update

Dependencies

This project forms the base from which to connect the network. Telecommunications allow users to access disparate databases, but if the elements in these databases are not common, the information will be useless to network users. Many projects are dependent upon successful implementation of statewide standards. These include:

- Statewide Automated Fingerprint Identification Systems
- Statewide Integrated Criminal History
- Magistrate System
- Statewide Identification Index
- Statewide Warrant System
- Courtroom Automation
- Statewide Juvenile Case Management Systems

Initial Cost Estimates

Role/Function	FTE[1]	Months	Total FTE Months	Total Cost[2]
Project Management	1	18	18	396,000
Facilitator	1	9	9	198,000
Analyst	2	18	36	792,000
Data Integration Expert	1	18	18	396,000
Justice Information Expert	1	9	9	198,000
Meeting Facilitation[3]	n/a[4]	n/a	n/a	120,000
Total			**90**	**$2,100,000**

[1] Full Time Equivalent

[2] One FTE is costed at $22,000 per month.

[3] Meeting facilitation costs include in-state travel and lodging costs for staff and committee members as well as miscellaneous administrative expenses.

[4] Not applicable

Ongoing (Data Quality Audit) Estimated Costs

Role/Function	FTE	Months	Total FTE Months	Total Cost
Audit Management	1	12	12	264,000
Audit Staff	2	12	24	528,000
Total			**36**	**$792,000**

CJIN NETWORK SECURITY

NEED TO CHANGE

- Criminal justice users require access to information from anywhere in the network.
- Connection of criminal justice systems to public networks creates a security risk.
- Data transmitted across the network is vulnerable to being intercepted and compromised.

RECOMMEND SOLUTIONS

- Develop and implement a CJIN network security plan.
- Define requirements for network security standards including network access control, authentication, and encryption.
- Review the security design and conduct a CJIN network security audit.
- Implement a CJIN security pilot including firewall-based access control, trusted third-party authentication, and data encryption.
- Assess the impact of CJIN security on overall CJIN network and end-users.

Current Situation

Current network security utilizes traditional system-based security. User accounts, logon IDs, and access profiles are used to grant or restrict access to systems, applications, and data. Access is generally restricted to workstations and PCs directly connected to host computers over a private network. Little or no end-user dial up access is supported on these systems. These private network systems provide adequate access control for the current base of users.

Recommendations

Implement a CJIN network security plan. CJIN security will be standards based and will include the following:

Validation of network access

Connection of CJIN to any public (non-CJIN) network will require the installation of network firewall systems. Firewall systems will guard against unauthorized access to the CJIN network. Commercial firewall products will be used to provide the necessary access control. Effective use of commercial firewall technology will be an important part of the overall CJIN network security plan.

User authentication

CJIN user authorization will be validated using conventional password-based security. A user will be required to enter a User ID and a password to gain access to a system or server. The user account and password will be verified before granting access to the system. The authorization step in CJIN security will be essentially the same as that of current system access controls. In addition to authorization security, CJIN will incorporate trusted third-party authentication. Trusted third-party authentication uses a secure system to validate the user's account and grant access to the requested

application. Third-party authentication can provide network-wide access with a single user logon. This will greatly simplify the administration of CJIN security.

Data encryption

CJIN network security will encrypt passwords, keys, and data. Both single key and double-key encryption will be used. Data Encryption Standard (DES) single-key encryption will be used for inter-process communications between servers. When single key encryption is used, both parties must know the same key before they can exchange encrypted messages. The over-the-air transmission of CJIN mobile data will be encrypted using DES. Double-key encryption, also known as public key/private key encryption, allows two parties to exchange encrypted data without requiring that each party be given the same key. The CJIN trusted third-party authentication process will use public key/private key encryption.

Network monitoring, security audits, planning, management, and administration

CJIN management will develop and maintain a security plan. Ongoing monitoring of the network will be performed by CJIN management. There will be a security audit performed to review the CJIN security plan and advise CJIN management of recommended changes or enhancements to the plan. The audit will include an analysis and review of the security pilot. The effectiveness and overall impact of the pilot will be studied. Changes to the CJIN security plan will be made following the pilot system audit. Ongoing management and administration of the CJIN network will be required. CJIN management may choose to create a special security "SWAT" team to advise CJIN management of new security threats that may arise.

Recommended Technology

CJIN will incorporate trusted third-party authentication. This authentication process, known as Kerberos security, was first developed at the Massachusetts Institute of Technology. Authentication software tools are commercially available

from RSA Data Security, Incorporated and other vendors. These tools will be used to develop a CJIN security system that will encrypt user passwords and authorization codes and will be used to send encrypted data over a public network.

CJIN will require special network security precautions. Firewalls, specialized software programs that reside in routers and dedicated servers, will be used to guard against unauthorized access to the CJIN network.

These technologies, together with conventional system security procedures, will be combined to secure the CJIN network form unauthorized access.

Benefits

- Effective CJIN network control
- Reduce the risk of unauthorized access to CJIN systems and data
- Network-wide access managed using a single user logon
- Protection and data integrity of sensitive CJIN information

Use of Kerberos-based authentication will require that the CJIN user workstation be able to locally execute a logon program as well as store and forward the resulting tickets and certificates. Mainframe terminals will not be able to execute a logon program. Custom mainframe software will have to be written to provide terminal support for Kerberos authentication. Alternately, CJIN users will require intelligent workstations to perform Kerberos security functions.

Existing CJIN applications will have to be modified to accept the resulting Kerberos tickets. This will require a significant amount of time and effort due to the large number of CJIN systems and applications that must be modified. Modifying and enhancing those existing applications that access criminal history data and other sensitive data will be the highest priority.

Risks

Firewall systems, because they unavoidably add another link to the network, may negatively impact CJIN network performance and throughput.

Kerberos security systems rely on conventional user passwords. These can be written down, copied, and readily compromised if standard system security practices are not enforced.

Authentication message traffic will increase overall CJIN network traffic. Minimizing authentication message traffic will require the use of time windows during which the workstation can dynamically generate new authentication codes without requiring accessing the trusted service. These time windows become an additional risk factor in the overall security design.

As inter-agency computing becomes a standard part of CJIN operations, member agencies will need to provide non-agency users with view-only as well as update access to existing applications and data. CJIN users equipped with powerful desktop computers will, over time, come to expect and demand unimpeded access to the information necessary to performing their assignments.

A special CJIN security SWAT team may be formed that will be comprised of members of the CJIN community, SIPS, and the IRMC. The SWAT team would be responsible for responding to all detected breaches in CJIN security. In addition, the SWAT team will advise CJIN management of new security threats that may arise.

Dependencies

Use of Kerberos-based authentication will require that the CJIN user workstation be able to locally execute a logon program as well as store and forward the resulting tickets and certificates. Mainframe terminals will not be able to execute a logon program. Custom mainframe software will have to be written to provide terminal support for Kerberos authentication. Alternately, CJIN users will require intelligent workstations to perform Kerberos security functions.

Existing CJIN applications will have to be modified for use with Kerberos authentication. This will require a significant amount of time and effort due to the large number of CJIN systems and applications that must be modified.

Initial Cost Estimates

Cost Components	Firewall System ($)	DCE Security Pilot	LEMS Kerberos Security ($)	Total ($)
Hardware	50,000[1]	50,000[2]	50,000[3]	150,000
Database	na[4]	30,000	na	30,000
Software Licensing	75,000[5]	10,000[6]	75,000[7]	160,000
Software Development	na	NSP[8]	275,000[9]	275,000
Software Implementation	27,500[10]	61,875[11]	137,500[12]	226,875
Project Management	5,500	13,750	68,750	88,000
Total	**$158,000**	**$165,625**	**$606,250**	**$929,875**

Ongoing Cost Estimates

Firewall technology will continue to evolve in response to the computer hackers developing new means of bypassing network security. Upgrading and maintaining CJIN firewall security will be an additional ongoing network expense.

Cost Components	Firewall System (Annual $)	DCE Security Pilot (Annual $)	LEMS Kerberos Security (Annual $)	Total (Annual $)
Maintenance	16,250[13]	11,000[14]	16,250	43,500
Line Charges	NSP	NSP	na	na
Training	na	NSP	na	na
Total	**$16,250**	**$11,000**	**$16,250**	**$43,500**

1. (5) firewall systems @ $10,000 per system hardware.
2. Estimated cost for authentication server.
3. Estimated cost for Kerberos server.
4. Not applicable.
5. (5) firewall software licenses @ $15,000 per system.

6. Estimated licensing cost @ $50 per user for 200 users.

7. Estimated licensing cost for Unisys mainframe Kerberos software.

8. Not separately priced. DCE security development costs are included in application costs.

9. Estimated 2000 hours @ $137.50 per hour.

10. Estimated 200 hours @ $137.50 per hour.

11. Estimated 450 hours @ $137.50 per hour.

12. Estimated 1000 hours @$137.50 hour.

13. 10% of hardware cost plus 15% of software cost.

14. 10% of hardware cost plus 15% of license cost and purchase cost of database, software.

CJIN TCP/IP NETWORK

NEED FOR CHANGE

- Current criminal justice computer systems use incompatible communications protocols.
- The state must maintain multiple separate user networks.
- Information cannot be readily accessed and exchanged between systems.
- End-user terminals cannot directly communicate with all of the different criminal justice systems.
- Current communications protocols cannot effectively support newer client-server applications.
- New users require access to information from public networks and common carriers, including dial-up and mobile access.
- New applications, such as a statewide AFIS system, will require a high-speed wide area network capable of supporting industry standard communications.

RECOMMENDED SOLUTIONS

- Develop a CJIN-wide Transmission Control Protocol/Internet Protocol (TCP/IP) network plan.
- Conduct a TCP/IP network pilot.
- Implement a statewide TCP/IP communications CJIN network.
- Implement TCP/IP protocols and services on all CJIN host systems.

Current Networks

The current criminal justice network environment consists of separate AOC, SBI, and SIPS networks. These networks have been designed to support the needs of each individual agency. The AOC and SBI networks have traditionally been based on proprietary vendor communications protocols. These networks are capable of exchanging and sharing information on a limited basis. Proprietary network terminals must use mainframe-based emulation services to access outside justice systems. Dedicated communications links are required to access and exchange information residing on these systems. The SBI, and to a lesser degree the AOC, have begun to support industry standard protocols including Transmission Control Protocol/Internet Protocol (TCP/IP). These agencies do not currently provide non-agency users with direct access to the information stored in these systems

Envisioned Network

The envisioned CJIN network will be a high speed wide-area communications network. CJIN network connections will be available at several different connection types and speeds. These service levels include the following:

CJIN User	**Small User I**	**Small User II**	**Medium User I**	**Medium User II**	**Large User I**	**Large User II**
Connection Type	14.4K Dial Up SLIP	56K SMDS	1.544 Mbit SMDS	10-20 Mbit ATM, PVC	45 Mbit DS-3 ATM, PVC	155 Mbit OC-3c ATM, PVC

Systems will be connected to the CJIN network using one of the defined service levels. CJIN agency mainframe systems at the SBI, AOC, and SIPS facilities will be connected to the network using Asynchronous Transfer Mode (ATM) switch technology. Central office ATM switches support OC-3c fiber optic links communicating at 155 Mbit per second speed. Premise ATM switches will support 45 Mbit per second DS-3 communications. Use of these connections for TCP/IP communications will initially be limited to 10 Mbit per second. Future ATM switching technology will support TCP/IP communications at up to the DS-3 rate of 45 Mbit per second.

The CJIN network will use TCP/IP communications. TCP/IP, an industry-standard suite of communications protocols and applications, will become the standard mechanism for CJIN information exchange. TCP/IP provides support for routing, packet exchange, message handling, file exchange, and interactive terminal services.

Mainframe systems, servers, and desktop systems will all communicate using TCP/IP. Desktop systems connected to departmental LANs (local area networks) will use TCP/IP to exchange information with CJIN host systems. Dial-up users, and mobile data users, will be able to use TCP/IP to access the CJIN network.

The CJIN network, a private network, will be able to be connected to public networks such as the North Carolina Information Highway (NCIH) and the Internet. CJIN users will be able to access systems and information that reside on the public networks. Network security firewall precautions will be in place to prevent unauthorized users from accessing the CJIN network. Kerberos security, a trusted third-party security process developed by MIT, will be implemented by CJIN to prevent unauthorized users from accessing CJIN data.

Benefits

The TCP/IP network will:

- allow users access to needed data regardless of its location.
- allow agency and departmental systems to have direct access to the CJIN network.
- support the vision of CJIN agencies sharing information.
- effectively merges three separate networks into one network.
- leverage the investment in the current state network architecture.
- utilize a range of the best technology offerings currently available.
- anticipate and support future user demands for more sophisticated access to CJIN information.
- provide support for turn-key Computer-Aided Dispatch systems for law enforcement to be connected to the network.
- provide support for newer graphical applications such as the AOC Case Management System, a graphical user interface (GUI) based Visual Basic application.
- provide a high-speed network capable of supporting a statewide AFIS system.
- provide the capacity to support future NCIC 2000 requirements for mugshots and fingerprints for warrants.

Network Cost Estimates - Sites / Locations

Cost Component	SBI / DCI	SIPS (DOC, DMV)	AOC
Capital Costs	$50,000	$50,000	$75,000
Annual Fees	$48,000	$48,000	$48,000

Network Cost Estimates - User Costs

Cost Component	Small User I	Small User II	Medium User I	Medium User II	Large User I	Large User II
Service Type	14.4K Dial Up SLIP	56K SMDS	1.544 Mbit SMDS, T1/DS-1	10-20 Mbit T3/DS-3 ATM[1] ,PVC	45 Mbit T3/DS-3 ATM, PVC	155 Mbit OC-3c ATM, PVC
Capital Cost (ANCHOR Net)	$400	$500	$1,700	$25,000	$35,000	$35-50,000
Monthly Cost	$35/mo	$850/mo	$2,500/mo	$9,600/mo[2] for each end point	$4,500/mo, plus inter-exchange carrier fees. Total estimated cost: $35,000/mo	$5,000/mo plus inter-exchange carrier fees. Total estimated cost: $80,000/mo

1. Requires a premise ATM switch, estimated cost: $25,000 or $4,000 per month. A central office ATM switch is also required for this level of service. The per-connection cost is $850 per month plus $500 installation.

2. Assumes one inter-LATA route. This will require an on-site service multiplexer or premise ATM switch. A 10 Mbit/sec PVC link, one not requiring an inter-LATA connection, will cost approximately $2,500 per month per site.

Initial Cost Estimates

Cost Components	Inter-Agency High Speed ATM Connection[1] ($)	Statewide Fingerprint Identification (SAFIS)[2] ($)	In-Court Automation[3] ($)	Magistrate System[4] ($)[5]	Identification Index / Criminal History ($)[6]	Total ($)
Capital Cost	175,000	170,000	170,000	100,000	850,000	**1,465,000**
Installation Cost	10,000	150,000	150,000	300,000	2,550,000	**3,160,000**
Total	**$185,000**	**$320,000**	**$320,000**	**$400,000**	**$3,400,000**	**$4,625,000**

Ongoing Cost Estimates

Cost Components	Inter-Agency High Speed ATM Connection (Annual $)	Statewide Fingerprint Identification (SAFIS) (Annual $)	In-Court Automation (Annual $)	Magistrate System (Annual $)	Identification Index / Criminal History (Annual $)	Total (Annual $)
Equipment Maintenance	17,500	17,000	17,000	10,000	85,000	**146,500**
Service Fees	1,260,000	3,000,000	3,000,000	2,040,000	4,335,000	**13,635,000**
Technical Support[7]	144,000	NSP	NSP	NSP	NSP	**144,000**
Total	**$1,421,500**	**$3,017,000**	**$3,017,000**	**$2,050,000**	**$4,420,000**	**$13,925,500**

1. Assumes that SBI, AOC, and SIPS computing centers are interconnected by a 45Mbit/sec ATM permanent virtual circuit.

2. Assumes that SAFIS sites will be connected to the SBI's AFIS computers via 1.544 Mbit/sec SMDS service.

3. Assumes that county court houses will be interconnected via 1.544 Mbit/sec SMDS service.

4. Assumes that magistrate workstations are connected to the AOC computer center via 56 Kbit/sec SMDS service.

5. Assume that network technical support for SAFIS, In-Court Automation, and Magistrate projects are not separately costed.

6. Assumes 1,700 workstations distributed over 425 sites, four workstations per site, connected via 56K SMDS service.

7. Assumes that technical support for application telecommunications is not separately priced (NSP).

CJIN END-USER TECHNOLOGY UPGRADE

CURRENT SITUATION

- The majority of criminal justice users still use mainframe terminals to access CJIN data.
- Existing PC workstations are primarily used to emulate mainframe terminals.
- Experienced PC users have ever-increasing expectations for technology.
- Future CJIN network access and security will require intelligent workstations.

RECOMMENDED SOLUTIONS

- Define requirements for a CJIN workstation including processor architecture, operating system, user interface, networking, applications, and security.
- Implement a CJIN workstation pilot.
- Implement CJIN end-user workstation technology.
- Assess results of workstation pilot and modify workstation solution as necessary.

Current Situation

The majority of criminal justice users currently access agency systems using terminals connected by a private network to a mainframe. In addition, PC workstations configured for terminal emulation are used to access CJIN systems. Existing workstation standards for information processing systems, as defined by National Crime Information Center (NCIC), are designed to meet only minimum requirements. Agencies are currently deploying PC workstations without the benefit of an organized CJIN workstation technology assessment.

The inter-agency exchange of information is rapidly evolving to extend to the desktop. CJIN agencies will need to provide outside users with controlled access to agency applications and data. CJIN users, who are becoming increasingly comfortable with personal computer technology at home and on the job, are expecting computer systems to provide them with unimpeded access to necessary information.

New network security programs will be executed on the local workstation. In addition, sensitive data will be encrypted at the source before being sent over the network. Encryption and de-encryption will be performed at the workstation.

Approach

Access to CJIN systems and data will require a powerful desktop workstation. This workstation must be capable of accessing CJIN data through the network and displaying the information in a format that can be readily understood by the user. Commercial software technology will be used to provide the necessary processing functions. In addition, CJIN security will perform user workstation authentication.

CJIN users will first request logon authorization by entering a user account and password. This user information will be validated by the local system or server. Kerberos authentication, a trusted thirty party authentication process developed at MIT, will then be initiated between the CJIN workstation and the network. This authentication process will require local processing capability by the CJIN workstation. The Kerberos process will provide application tickets to the workstation that will allow the user to access necessary information.

Once authentication has been completed, the CJIN user will have access to the necessary CJIN systems and data. The user will select the requested system from a menu. The workstation will automatically connect the user with the requested application. The user will not be required to know the location of the application or data.

CJIN information will be retrieved to the desktop and presented to the user. Information may be reformatted using a workstation based end-user application. The graphical user interface of the CJIN workstation will enable the end-user organization to develop customized applications for processing CJIN information. Alternately, users will use terminal emulation software residing on the workstation to access CJIN information residing in agency systems.

End-user workstation technology will change the following CJIN business processes:

- **Intelligent workstations will enable users to directly access the CJIN network.**

  Users will not be required to go through the mainframe to access CJIN data. User workstations, connected to high-speed local area networks, will directly access the CJIN wide-area network. Future client-server applications will be workstation based.

- **CJIN workstations will execute Kerberos security authentication software**.

  Kerberos security will allow CJIN users to access multiple applications without requiring separate logons.

- **Existing applications may have to be modified to implement Kerberos security**.

  New applications will be designed to utilize Kerberos authentication. Existing applications will be modified on an as needed basis. Applications that access sensitive CJIN data will be enhanced with Kerberos security.

CJIN end-user workstation technology will meet the following criteria:

- Use a scalable microprocessor architecture.
- Provide a modular, end-user configured system based on commercially available technologies.
- Employ standards-based software for the operating system, user interface, network access, application interface, and security.
- Provide direct user access to the CJIN network and data.
- Provide workstation support for Kerberos-based network security.

Recommended Technology

CJIN workstations will be commercial microcomputers systems configured with industry-standard software. These workstations will connect to the CJIN network via a LAN connection. In addition, workstations will be able to use dial-up connections to access the CJIN network.

A CJIN workstation pilot will be performed to select the microcomputer architecture for the workstation. The following microprocessor architectures are recommended for consideration:

- Intel P5 (Pentium) technology
- Intel P6 (Next generation Pentium) technology

- DEC Alpha technology
- PowerPC technology
- MIPS technology

The CJIN workstation will use an industry standard operating system. The following operating systems are recommended for consideration:

- Microsoft Windows 95
- IBM OS/2

A CJIN workstation pilot will be performed to evaluate alternative workstation solutions. Competitive forces in the marketplace will determine the relative price performance of these technologies. The CJIN workstation solution will provide for an upgrade path during the implementation cycle. Microprocessor technology can be expected to continue to evolve at such an accelerated pace that no meaningful selection can be performed until just prior to implementation. As an example, the original NCIC 2000 workstation guideline required an Intel 80386 processor and 4 MB of RAM memory. Organizations that adopted the NCIC specification as a standard are already faced with upgrading these systems. Only by selecting a workstation architecture that is both modular and scalable will CJIN be able to minimize premature workstation obsolescence.

Initial Costs

CJIN end-user workstation technology costs will be determined by the market costs of the following component technologies:

- Central processor unit and core system
- Computer memory
- Local disk storage
- Display monitor and controller
- Network interface adapter
- System software including operating system software, network software, and security software

The following cost table is an example of estimated costs for this technology today:

Component	Description	Cost
Central processor and core system	Intel 75 MHZ Pentium CPU	$1,200.00
Computer memory	32 MB of RAM	$1,350.00
Local Disk Storage	540 MB[1]	$300.00
Display monitor and controller	17 inch color display and controller	$1,000.00
Network interface adapter	Network Interface Card	$200.00
System software	Windows 95, TCP/IP, Kerberos, or RSA, licenses[2]	$950.00
Total		**$5,000.00**

[1] One Gigabyte disk drives may be needed in the future for some stations. This would increase the cost of disk storage from $300 to $700 per workstation.

[2] If a full office automation software suite is required, the per workstation cost will increase by approximately $450.

While the cost of specific computer technologies will continue to fall, overall system costs can be expected to remain fairly constant. In the future, as the price to performance ratio of computer hardware continues to improve, CJIN will benefit from the enhanced performance and capabilities of these newer technologies.

Initial Cost Estimates

Cost Component	Unit Cost ($)	Magistrate Project ($)	In-Court Automation Project ($)	Identification Index / Criminal History Workstations ($)
Workstation Hardware	4,300	860,000[3]	6,665,000[4]	7,310,000[5]
Workstation Software	700	140,000	1,085,000	1,190,000
Related Server Costs	na	NSP[6]	2,700,000[7]	na

[3] (200) magistrate workstations

[4] Assumes (310) court rooms, (5) workstations per court room.

[5] Assumes 1700 criminal history workstations will replace existing PIN terminals.

[6] Not separately priced. Project management costs included in overall project cost.

[7] Assumes (90) additional mid-level file servers @ $30,000. Currently (10) server installations are in progress.

Cost Component	Unit Cost ($)	Magistrate Project ($)	In-Court Automation Project ($)	Identification Index / Criminal History Workstations ($)
Related Printer Costs	2,400	480,000[8]	744,000[9]	na
Project Management	na	NSP	NSP	NSP
Total	**$7,400**	**$1,480,000**	**$11,194,000**	**$8,500,000**

Ongoing costs of CJIN end-user workstation technology will include the following:

- Hardware maintenance

  A maintenance program with provision for swap-out replacement for workstation components will be required.

- Software upgrades

[8] Assumes (200) duplex laser printers @ $2,400.

[9] Assumes (310) duplex laser printers @ $2,400.

Software upgrades will be periodically required. Site licenses for software may be cost effective for CJIN. Automated distribution and management software will enable CJIN workstation software to be centrally managed and disseminated.

- User training

  Users will require workstation and application training. In addition, user training for CJIN security procedures will be required.

- Help desk support

  Ongoing user support will include a help desk to answer questions and solve user problems.

- Technology upgrade programs

  Deployment of end-user workstations will require an ongoing upgrade program. Newer workstation technologies, offering better performance and end-user capabilities, will be used to supplant and replace existing workstations.

Ongoing Cost Estimates

Cost Components	Unit Cost (Annual $)	Magistrate Project (Annual $)	In-Court Automation Project (Annual $)	Criminal History Workstations (Annual $)
Hardware Maintenance[10]	344	107,200	592,720	584,800
Software Maintenance[11]	105	21,000	162,750	178,500
Server Maintenance[12]	na	NSP	270,000	NSP
Total	**$449**	**$128,200**	**$1,025,470**	**$763,300**

[10] Hardware maintenance estimated @ 8% of initial hardware cost, per year.

[11] Software maintenance estimated @ 15% of initial software cost, per year.

[12] Server maintenance estimated @ 10% of initial server cost, per year.

Quality Assurance

The end-user technology pilot will provide independent validation and verification of the chosen workstation technology. The pilot team, using the selected hardware and software components, will create a working prototype of the CJIN workstation environment. This prototype will be developed in close coordination with the CJIN network and CJIN security projects.

Once the prototype has been completed, a pilot evaluation program will begin. The pilot will test the functionality, performance, and reliability of the CJIN workstation in a production environment. Upgrades and replacements to the components used in the pilot workstation will be incorporated into the final pilot assessment.

End-user workstation technology will be deployed in stages. Initial users, as early implementors, will be among the first to benefit from these new systems. In the later stages, users will benefit from the knowledge gained during earlier implementations. Quality assurance procedures defined in the earlier stages will be continually refined. In addition, advances in microcomputer technology will provide enhanced capability and performance.

STATEWIDE MOBILE VOICE AND DATA SYSTEM

CURRENT SITUATION

Incompatible radio equipment is inhibiting interagency communications in routine and emergency situations. A lack of statewide guidance and standards in radio communication technology fosters discordance and escalates the cost of providing communications statewide. In addition, FCC frequency refarming proposals may inevitably force the state to replace most of its transmitters and radios.

RECOMMENDED SOLUTION

By the end of 1997, award a contract for the implementation of a statewide mobile voice and data radio network. The network should be completed by the end of 2005; and be compliant with the APCO 25 standards project. The state should:

- Commit funding to provide the infrastructure for mobile voice and data coverage statewide while cities / counties should complement the efforts with capacity to meet urban, industrial, and portable requirements.
- Develop implementation plans on a county-by-county basis, optimizing each county's need for portable and in-building coverage with the state plan for mobile communications.
- Provide mobile data terminal access to the full CJIN network using the Mobile Data Pilot (MODAP) as a baseline.
- In the near term, conduct a frequency identification study and expand the MODAP pilot program to address the issues of security and performance.

A goal of the CJIN study was to "develop a plan for a statewide wireless integrated law enforcement communication system, including voice and mobile data terminals, and to study the costs of making that system available to local governments." This section discusses the need for a statewide wireless communication system and makes recommendations on an approach which should achieve county buy-in while leveraging the counties' existing expertise and investment in 80MHz trunking technology.

This section is organized as follows:

Background

Current Situation
- The Impact of FCC Initiatives to Refarm the Private Land Mobile Frequency Bands
- Status of APCO 25 Effort
- Current Investment in 800MHz Trunking Technology
- Cost to Implement a Statewide Network Mobile Voice and Data Network

Mobile Voice and Data Requirements
- Geographic Requirements
- Data Communications Requirements
- Interoperability
- Administrative Requirements

Technology Alternatives
- 450 MHZ Trunking Systems
- Summary of Emerging Trends in Wireless Technology: TDMA, GSM, and CDMA
- Personal Communications Services (PCS)
- Mobile Data Alternatives

- Mobile Voice and Data Standards

Implementation Alternatives

Approach
- Goals
- Objectives
- Governance
- Mobile Data Strategy
- Guidelines for State / County Cost Sharing
- Ongoing Costs
- Allocation of Funds

Implementation Tasks
- Frequency Identification Study
- Expansion of the MODAP Pilot
- County Planning Study
- Issue Implementation Contracts

Benefits
Risks
Vendor Contacts

Background

The purpose of this section is to introduce the reader to significant organizations and activities related to radio communications in North Carolina.

Associated Public-Safety Communications Officials, International Incorporated (APCO) - APCO serves as the frequency coordinator for public safety and special emergency 800MHz spectrum. The APCO 25 project is an initiative to define standards for digital radio equipment for public safety officials.

Federal Communications Commission (FCC) - The federal organization responsible for allocation and monitoring of radio frequencies.

Chronology of FCC Related Events	
December, 1983	U.S. Congress directed the FCC to establish a plan that would ensure the communications needs of state and local public safety authorities would be met
July, 1986	FCC adopts service rules and technical standards for the 821-824/866-869MHz bands
December, 1987	FCC adopts national plan for public safety services
February, 1989	North Carolina Regional Communications Planning Committee is formed
November, 1991	North Carolina Regional 800MHz Communication Plan (Region 31 Plan) is submitted to the FCC
March, 1993	Resubmission of the Region 31 Plan

North Carolina Regional Communications Planning Committee (NCRCPC)- Authored the Region 31 Plan for use of the NPSPAC channels, March 1993.

National Public Safety Planning Advisory Committee (NPSPAC) - NPSPAC is an open membership committee which enables the public safety community and the public to participate in spectrum management through recommendations on policy, technical standards, and procedures to satisfy long-term public requirements. Based on NPSPAC's report, the FCC allocated the 821-824/866-869 MHZ bands (often called the NPSPAC channels) for public safety use, and adopted policies, procedures and rules that constitute a national plan for public safety services. Additionally, the national plan specified that regional plans would be developed before frequencies would be allocated. This process in now closed with the adoption of the plan by the FCC. Recent events have revealed that there should have been a procedure for updates and changes.

North Carolina Smartnet Users' Network (NCSUN) - A users group consisting of Motorola Smartnet users. NCSUN currently has agreements in place to provide trunking among the users.

State Information Processing Services Division (SIPS) - Functions as the North Carolina primary frequency advisor for APCO. SIPS has provided technical services and leadership in the area of wireless communications for the state. They have an existing contract with Motorola to provide 800MHz trunking radio services in the Triangle and many other locations throughout the state. The contract covers a 10-channel 800MHz trunked radio system that is FCC licensed to Statewide Telecommunications Services(STS) for the Triangle area, plus 20 Motorola owned sites across the state, and a minimum of three talk groups on each of the NCSUN 800MHz local government owned systems.

Statewide Interagency Public Safety (SWIPS) Radio Communications Plan - An interagency plan, which directly preceded and formed the basis for many of the radio communications recommendations in this study.

Current Situation

Radio technology is a fundamental tool of law enforcement and public safety. Estimates set the number of radios in use in public safety statewide as high as 75,000 units. For officers on patrol, the radio is the sole means of communications to obtain assistance in life threatening situations and, more routinely, the primary mechanism for dispatch. Similar dependency on radio communication is echoed throughout public safety and law enforcement organizations.

The existing statewide radio communications infrastructure is based on technology which is over forty years old and is extremely limited in capability compared to present technology. In public safety radio communications, the state currently faces the following challenges:

- State officials are often unable to communicate with local agencies.
- Local agencies communications are often ineffectual in the following situations:
  - county to neighboring county
  - city to county
  - agency to agency
- Current and planned investments in incompatible technologies will exacerbate the above problems well into the next century unless statewide action is taken now.
- Smaller counties lack the technical and financial resources to effectively procure and manage the 800MHz trunking technology infrastructure.

The state-of-the-art for radio technology today is based on 800 MHZ trunking technology. Trunking enables many users to share a few channels by using technology which is similar to that in use by telephone systems. When a user makes a call, a trunk line is assigned to that user for the duration of the call. At the completion of the call, the trunk line is freed for the next user. In this environment, capacity only becomes a problem when the number of users who want to make calls at any one instance exceeds the number of trunked lines.

Since in a radio environment, the average transmission is five to six seconds, trunking enables numerous users the ability to use only a few channels. As a guideline, each channel in a trunked environment will support up to 100 users in typical public safety applications as compared to 70 users for conventional channels. Trunking technology is so effective that the FCC and the NCRCPC specify that all communication systems which utilize five or more channels be required to operate in a trunked configuration.

The FCC's auctioning of radio frequencies has placed local and state governments in a position where they are now competing for channel frequencies with private enterprise. Given the finite number of frequencies available and the demand from the public sector, it is becoming increasingly difficult to license frequencies for public safety usage. This expansion increases the need of local and state governments to conserve and share frequency whenever possible.

Impact of FCC Initiatives to Refarm the Private Land Mobile Frequency Bands

One driving force which is substantiating a need for immediate action is the FCC refarming proceeding of frequencies below 512MHz. Refarming is a complex undertaking by the FCC's Private Radio Bureau. It is a plan to attain more efficient spectrum usage through implementation of narrow band technology thus creating more channels and reducing interference.

According to the FCC, the purpose of the proceeding is "to increase channel capacity in these bands, to promote more efficient use of these channels, and to simplify our policies governing the use of the bands by a wide variety of small and large businesses and public safety agencies throughout this nation."

The specific proposals include:

1) having the licensees move to spectrum efficient standards by generally reducing channels from the current 25KHz spacing to 6.25KHz, increasing capacity by 300 to 500%.
2) employing a market-based approach called "Exclusive Use Overlay" through concurrence of existing users and permit centralized trunking.

3) consolidating the current 19 radio services.
4) significantly reducing permissible transmitting power levels and frequency deviation, thus creating efficient geographic co-channel reuse.

The objective to use spectrum more efficiently is assuredly commendable and yields long term benefits. For the current user of the spectrum below 512MHz, the costs to continue operation will be expensive, perhaps even more costly than to revamp or acquire an 800MHz system. The refarming rules are still a proposal. However, it is anticipated that the FCC refarming proposals will require significant changes in technology in the 2006 time frame and replacement of all technology by 2012. The actual dockets are anticipated in the later half of 1995. The new FCC requirements are anticipated to substantially render obsolete all existing radio technology subject to grandfathering of the equipment. There is no impact on 800MHz channels.

Status of APCO 25 Effort

The activity that has resulted in the APCO 25 document is now approaching a milestone. The existing effort is anticipated to end its working sessions at the summer annual conference of the APCO officials meeting. With the completion of the working effort, the completed documents are expected to be issued sometime during the first quarter of 1996. The next phase of the activity will be to continue to address several other issues. Including the migration to 6.25KHz channel spacing and Time Division Multiple Access (TDMA). When, and in what form, that part of the APCO project will take is difficult, if not impossible to predict.

Current Investment in 800MHz Trunking Technology

On a statewide basis, there has already been a significant investment in 800MHz radio technology. While cost figures are hard to tally, existing investment by local governments can be estimated at $75 to $100 million. Unfortunately, without a statewide policy, local governments are moving in directions which are incompatible and inhibit integration of communication systems. It is important to remember that the tax payers are already financing this technology, regardless of whether this funding is coming from state or local sources.

The following chart identifies some of the current and planned coverage of 800MHz trunked systems. The analysis was performed on a county-by-county basis even though the coverage may only be for a municipality within the county. The major metropolitan areas have been included even though full county coverage is unknown.

Area / Region	Population 1994	Technology	Comments	Investment (Millions)
Alamance County Burlington	112,776		Consultant study completed for a city / county system	
Buncombe County Asheville	183,392	Motorola	5 Channel, 500 Units	$2.5
Catawba County Hickory	124,634	Ericsson G.E.	On line April 1, 1995	$1.7
Craven County New Bern	87,059	Motorola	5 Channels, requesting 6 more	
Cumberland County Fayetteville	84,000		Bid Advertised, response in May 1995,Public utilities system in operation	
Durham County Durham	195,506	Motorola	On line July 1, 1995	$8.0
Edgecombe County Rocky Mount Tarboro	57,190	Motorola	Rocky Mount has a six channel system	$0.8

Area / Region	Population 1994	Technology	Comments	Investment (Millions)
Forsyth County Winston-Salem	275,551		In-capital improvement program FY98	$10.0
Guilford County Greensboro, High Point	361,898	Motorola	Recently Awarded, 5 Site, Simulcast	$9.0
Harnett County Dunn	72,125	Ericsson G.E.	225 Units	$0.6
Johnston County	89,024	Ericsson G.E.	Operates off of shared repeater	$0.1
Mecklenburg County Charlotte	562,129	Motorola	28 Channels, Smartzone may expand to Gaston and Union Counties	$26.0
New Hanover County Wilmington	131,032	Motorola	5 Channels, Estimated order by June 1995, Leasing the system	$1.1
Rowan County Salisbury	115,935	Motorola		$3.0
Wake County Cary	486,158	Motorola	6 Channels, plans for 2 more, 480 Units, serves Morrisville PD	$1.7
Wilson County	67,688	E.F. Johnson	150 Units	$0.2
Duke University		Motorola	10 Channel System	$1.4
RDU International Airport		Motorola	132 mobiles / portables	$1.0

Area / Region	Population 1994	Technology	Comments	Investment (Millions)
TOTAL	**3,006,097**			**$67.1**

Population data is based on 1994 projections from the North Carolina Office of State Planning.

Cost to Implement a Statewide Network Mobile Voice and Data Network

The total costs to implement a statewide mobile voice and data network which serves the full needs of law enforcement, public safety, and state and local governments, is presented in the following chart. These estimates were determined based on experience in other states, review of the North Carolina project, and through discussions with vendors. These estimates are not based on a user requirements study or a competitive bid. However, they are felt to be indicative of

approximate costs.

Equipment	Unit Cost	Quantity	Subtotal
Trunked Repeater Stations	$20,000	3,400	$68,000,000
Convention Repeater for Mutual Aid	$15,000	320	$4,800,000
Trunking Controller	$300,000	80	$24,000,000
System Manager	$180,000	80	$14,400,000
Dispatch System Voice	$100,000	80	$8,000,000
Digital/Analog Voting Comparator	$10,000	80	$800,000
Repeater Antenna Systems	$35,000	160	$5,600,000
Microwave Link Upgrade	$10,000,000	1	$10,000,000
Radio towers	$400,000	35	$14,000,000
Equipment Building	$100,000	35	$3,500,000
Emergency Generator	$100,000	35	$3,500,000
Inter-Zone Overlay	$115,000,000	1	$115,000,000
Vehicle Radio	$3,500	25,000	$87,500,000
Portable Radio	$3,000	50,000	$150,000,000
Mobile Data System	$6,500	10,000	$65,000,000
Data Switch	$2,000,000	1	$2,000,000
Data Controller	$125,000	4	$500,000
Total Equipment			*$576,600,000*
Technical Assistance @10% of Total			*$57,660,000*
Grand Total			**$634,260,000**

The cost for the infrastructure is estimated at $241 million and is corroborated by the $187 million for the infrastructure procurement which was recently awarded by the state of Michigan. The Michigan infrastructure only provides mobile

coverage but includes 181 towers.

Mobile Voice and Data Requirements

Requirements for a statewide mobile voice and data system need to be considered from a variety of perspectives including:

- voice
- data
- geographic
- portable or mobile
- in-building coverage
- interoperability
- operational and tactical

This section elaborates on these requirements from a general perspective. Each county, city, or agency is likely to have unique preferences for radio service. Other sources of information on requirements can be obtained by reviewing the documentation of the Statewide Interagency Public Safety (SWIPS) Radio Communications Study.

Voice Communication Requirements

Each organization needs the ability to communicate among talk-groups within their own organization, such as a sheriff's office, police department, highway patrol, and fire department. Each of these organizations needs to be able to communicate with their dispatch and among each user to conduct daily business. On a routine basis, one agency has little need or desire to know the daily business of another agency. For instance the fire department is not concerned whether or not a warrant has been served.

Nonetheless, one of the key driving forces behind the requirement for shared communications is the need for multiple

agencies (fire, police, highway patrol, emergency management, among others) to communicate with each other in the event of a emergency, or in other situations requiring multi-agency response.

Geographic Requirements

Where the communications take place also impacts the design and cost of the system. Factors which affect these costs include:

- In-vehicle requirements (mobile)
- Outside the vehicle requirements (portable)

Mobile (car mounted) communications equipment works at a higher power rating than portable (hand-held) communications equipment, typically 35 watts versus 3 watts for portable equipment. As a result, the distance between the tower and the unit can be significantly greater in a mobile environment than in a portable environment. In other words, costs increase for portable coverage.

To extend coverage from a vehicle to a portable which may be in range of the car but out of range of the tower, a repeater may be installed in the car. However, several shortcomings in existing technology have contributed to an aura of unreliability in this technology. Unreliability is primarily due to a situation where multiple users are in the same vicinity as multiple repeaters and each of the repeaters attempts to retransmit the transmission. This problem can be mitigated by marrying the portable to the vehicle utilizing selective tones or addressing.

Additional power requirements are imposed when the user intends to use the portable equipment inside buildings or houses. Radio communications inside buildings is important in a number of public safety situations, particularly in the case of fire or an organized drug raid in an apartment building. As a result, urban and industrial areas are likely to require denser coverage.

North Carolina has a variety of terrain requirements, including mountains, hills, coastal regions, large urban areas, and vastly disparate rural areas. Each one of these environments creates new challenges in the design and deployment of radio technology.

Data Communications Requirements

Second only to the need for voice communication requirements among law enforcement officials in the field, is the need for data communications, such as:

- Drivers License and Registration Checks
- Missing Persons Checks
- Wanted Checks
- Hot File Checks
- Criminal Case History

Additional information requirements are being proposed by the NCIC 2000 initiative which identifies technology where fingerprint and image information will be provided via radio communications to officers in the vehicle.

Before much of this information can be transferred via the network, security issues must first be addressed. See the CJIN Security Project, Section VI.2 for more information.

Communication protocol requirements include TCP/IP communications with the CJIN network and SNA communications with legacy systems. In addition, requirements for integrated Automated Vehicle Location (AVL) and Global Positioning System (GPS) capability to provide automated vehicle location and tracking have also been identified.

The use of this technology was highlighted in the MODAP pilot which should serve as a basis for all data communication requirements in law enforcement statewide.

Interoperability

Interoperability is the ability to provide rapid and effective communications for a radio functioning within or outside its own system. A capability of a radio operated by a member at the state, county, or municipality level is to communicate directly with another. The dynamics of the public safety environment mandate this capability.

An often cited example of the Interoperability requirement is the stopping of a suspect vehicle by a State Highway Patrol Officer. Currently, the officer is solely in radio contact with his respective dispatching center unless a fellow officer happens to be in proximity. Interoperability will enable this officer to be in voice contact with law enforcement officers on patrol in the vicinity, i.e. municipal police officers or sheriff deputies, and thus facilitate timely assistance. Similarly, it enables units from different or adjoining jurisdictions to communicate directly during joint operations. The benefits are easily envisioned in the precarious conduct of a vehicle pursuit traversing multiple jurisdictions.

Disaster recovery operations are faced with the dilemma where agencies in the same jurisdiction are unable to talk to each other. During major disasters, widespread or localized, this is the most critical, single barrier to effective and efficient delivery of services. It is essential for units to talk directly to participating law enforcement, fire, rescue, and public works / utilities to ensure clear and safe traffic lanes, that streets and highways are cleared of debris, and that requests for help and resources are rapidly and properly deployed.

Managers of the agencies involved require communications for coordination of efforts. Only a statewide network can achieve the required results.

Administrative Requirements

Several organizational and administrative requirements are also imposed on the system. For instance, multiple channels will need to be designated for specific types of command and control for emergency response agencies. In addition, solutions for tactical situations will need to be considered on an agency by agency basis. The network will be required to operate 24 hours-a-day, 7 days-a-week.

Technology Alternatives

450 MHZ Trunking Systems

One alternative to 800MHz trunking systems is 450MHz trunking systems. This technology theoretically can provide a 30 to 40% improvement in coverage with all other factors being equal. Statewide, this could mean significant savings. Unfortunately, the availability of channels in the 30 - 470MHz frequency range are limited and clear channels are no longer available. Further complicating use of these frequencies is an absence of vendors providing trunking technologies in these bands.

Summary of Emerging Trends in Wireless Technology: TDMA, GSM, and CDMA

In the U.S., the primary decision each of the two licensed cellular telephone providers in each service area must make is which of three systems to adopt: TDMA, GSM, or CDMA. TDMA (time-division multiple access) allows three simultaneous conversations on a single channel that today supports a single conversation; advanced versions of TDMA allow up to six conversations on a single channel. TDMA technology is an evolutionary technology that is already in use in some markets in response to customer demand.

Groupe Speciale Mobile (GSM) is the European digital TDMA standard and is gaining acceptance in the Pacific Rim. In the past it was not popular in the U.S., but it is now gaining more consideration because of the widespread availability of GSM equipment. GSM received another boost with the MCIs' purchase of an interest in NexTel Communications Inc., the largest U.S. specialized mobile radio (SMR) carrier, which is converting to GSM. SMR provides an important alternative to traditional cellular systems, especially for fleet applications.

Most of Europe appears committed to GSM; while, the French GSM market has experienced fairly slow growth as has the GSM market in the U.K. The Middle East and Gulf countries are implementing GSM. Two national GSM operators have been licensed in South Africa, and Russia is setting up 12 regional GSM networks.

CDMA (code-division multiple access) uses a different technology to allow up to ten times the number of users on a set of frequencies. Rather than being implemented channel-by-channel, CDMA must be implemented across a large set of channels simultaneously. Although many companies have announced plans to adopt CDMA technology, initial CDMA service will not be available until late 1995. This delay means that even if CDMA ultimately becomes the dominant technology, carriers may be forced to adopt TDMA or GSM in the interim to provide capacity for immediate growing demand.

Personal Communications Services (PCS)

Several systems have been developed and implemented to provide PCS services. The most common is CT-2 (Cordless Telephone 2), which uses Frequency Division Multiple Access (FDMA). It provides less functionality, range, and coverage than does cellular radio, but generally has lighter weight, less expensive handsets, and lower carrier charges. Canada has mandated an advanced version called CT-2 Plus that is more complex, but offers more features. Many countries in Europe and Asia have adopted CT-2 as a standard.

One option for PCS is microcell CDMA technology, allowing a full range of digital communication, including data, fax, and voice. Microcells are typically several hundred feet on each side compared to conventional cellular cells that are several miles on each side. Microcells allow low power operation and high capacity through more sharing, resulting in lighter handsets, longer battery life, and smaller and less expensive cell sites. However, in the U.S., geographical coverage and mobility is crucial, and the hundreds of microcells required for this coverage may be no more economical than fewer macrocells. The economical solution is a mix of microcells and macrocells depending on density, an option that is available to conventional cellular technology as well.

Mobile Data Alternatives

When providing the capability for mobile data, there are several alternatives. The following table identifies the major alternatives available today and discusses the advantages and disadvantages of each of those alternatives.

Technology	Description	Advantages	Disadvantages
Piggyback data system on top of statewide 800MHz voice trunking system.	Either use the APCO 25 standards for data transmission or allocate specific channels for data. Data rates up to 9.6 - 19.2 Kbps for dedicated channel.	May be piggybacked on 800MHz voice backbone relatively inexpensively (10% to 15% of voice infrastructure costs). Fixed cost for infrastructure. Could achieve coverage statewide.	Large capital investment in infrastructure is required. Technology upgrades and management will be a large concern.
ARDIS	Currently 4.8Kbps, upgrading to 19.2Kbps. Covers more than 400 metropolitan areas and more than 10,700 cities and towns (80% of U.S. population). Has 1300 base station in U.S., approximately 25 in North Carolina. Good in-building coverage in major cities. Claims 35,000 users nationwide.	Low capital investment	Additional security concerns. Currently has low baud rate. Does not address voice requirements. Statewide coverage is at the discretion of the vendor. Coverage in rural areas is not planned and is unlikely. Per packet billing will be hard to manage and control. No plans for flat rate billing.
RAM Mobile Data	Per packet billing. Seamless roaming. 8Kbps now planning upgrade to 19.2. Estimated actual throughput is 2Kbps now and 13Kbps when upgraded. Coverage includes over 6000 cities and towns and 90% of urban population. Claims 17,000 users, 840 base stations. Mobitex technology supplied by Ericsson.	Low capital investment. Claims for good in-building coverage (area dependent).	Additional security concerns. Currently has low baud rate. Does not address voice requirements. Statewide coverage is at the discretion of the vendor. Per packet billing will be hard to manage and control.

Technology	Description	Advantages	Disadvantages
Cellular Digital Packet Data (CDPD)	19.2Kbps without compression Under development in NC. Only Charlotte covered. Have virtual connection, pay by the byte. Rate plans not available yet. Supports voice and data. Uses cellular's existing spectrum.	Low capital investment. Only need to invest in vehicle equipment. Only pay for information which flows through the network enabling the user to always stay connected.	Requires relatively expensive packet radio modems. Borrows cellular voice channels. Voice not allowed for dispatch purposes per FCC regulations.
Dial-Up Modems over Analog Cellular Voice Channels	Large files, uses public telephone lines pay whether or not we are moving data. Line charges. Designed for voice. Adequate for long files.	Up to 56.7Kbps using MNP on the modems. Uses public lines. Can be used just like regular modems.	Dial in line charges are assessed during connection, whether or not data is being moved.

Mobile Voice and Data Standards

There are a variety of emerging standards in wireless mobile communications. The basis and the potential for each of these standards at this point is speculative. The most heated debate currently is whether or not to support the APCO 25 project. The APCO 25 project specifies standards for digital trunking radio in the 800MHz range.

The objectives of the Project 25 Standards were "selected are to best fit public safety users' needs for 1) multi-source procurement; 2) interoperability; and 3) graceful migration"[1]

There are currently five vendors supporting the APCO 25 project standards, however, with the exception of Motorola, most of the vendors supporting the standards are new entrants or minor players in the field of SMR. This battle is still in

[1] Open Letter to the APCO Membership from the Project 25 Steering Committee, March 1995 APCO Bulletin

process and will probably be debated for the next few years. With industry acceptance, the APCO 25 project holds great promise to reduce the costs of radios and the radio infrastructure. However, full industry acceptance is speculative. Therefore, it is recommended that as North Carolina moves towards procurements during the RFP process, the standards be reevaluated to determine which will provide the state with the highest value performance and the most favorable life cycle cost. The question which needs to be addressed is how have the standards reduced the cost and improved the quality of the available products and services. If the standards fail to demonstrate an advantage, they should not arbitrarily be imposed. Nonetheless, North Carolina is taking a leadership position in this endeavor and may not yield the full benefits from the standards.

Implementation Alternatives

The recommended approach is for the state is to commit to a full statewide mobile voice and data solution with portable and in-building coverage considered on a county by county basis. This approach, which is recommend in Section VII, is the only feasible solution which meets the requirements of a statewide integrated system and will provide the best long-tem value. The remainder of this section presents three alternative approaches for implementation which also need to be considered. These alternatives are not mutually exclusive and may be incorporated into the state approach. The alternatives are:

- Issue statewide standards which are mandated
- Issue a procurement which all counties can use voluntarily
- Fill in the gaps between existing systems and along major highways

Mandate statewide standards for mobile voice and data.

In this alternative a statewide standard for mobile voice and data will be determined by a subcommittee of the IRMC. All state and local organizations will be required to adhere to those standards as they implement 800MHz systems. These standards will address the issue of compatibility, however there will be no incentive for organizations to add the additional infrastructure necessary to support state functions. The disadvantage of this approach is that counties are likely to reject any standards which add to system costs while providing minimal added value to the county perspective even though the state benefits may be significant. Further, this strategy may be considered as an unfunded mandate which is likely to cause considerable distress to local agencies.

Issue a procurement which counties and municipalities can use to purchase equipment.

With this alternative, the state issues a procurement which each county can use to purchase equipment. With this approach, counties are guaranteed to get compatibility with each other and are not required to conduct their own procurement process. In addition, there may be some cost savings because of the volume. The disadvantage is that there is no incentive for the counties to use the procurement (unless it becomes mandatory) and that counties may not be planning to provide sufficient resources for state usage. Further, there will be unclear policies on integration issues or there will be no incentive to support the integration among local and state agencies. Counties are likely to be concerned with how much they will charge the state and state issues will not be a priority.

Fill in the gaps between existing systems and along major highways.

The objective of this approach is to fill in the gaps along the busiest highways and between the major metropolitan area and foregoes adhering to the emerging APCO 25 standards. The advantage of this strategy is that existing defacto standards could be used for implementation, and the implementation costs will be relatively small in comparison to full statewide implementation. However, this strategy serves best those areas which are in high growth regions and has little regard for lower density counties on the outskirts of the state which also need infrastructure. Further, over the long term it will tie

the state to a single vendor which may result in high unit costs. In addition, if the state ever commits to statewide

implementation, the cost may be driven higher by the vendor since they will have an irreversible lock on the infrastructure.

Approach

This section establishes the goals and objective of the mobile voice and data initiative. It describes a governance model, discusses the mobile data strategy, and describes a cost model which may be used as a guideline for achieving local buy-in to the plan.

Goals

The state of North Carolina requires a cohesive and cooperative approach for the implementation of a total coverage, seamless, statewide radio voice and data communications system. The goals of this effort are:

- Identification of frequencies for use in the statewide network by June 1995.
- By the end of 1997, a contract should be in place which will enable implementation of a statewide mobile voice and data radio network.
- By the year 2002, all public service radio technology should be compliant with statewide standards.
- The statewide mobile voice and data network should be completely implemented by the end of 2005.

Objectives

In achieving these goals, several objectives are sought:

- Counties without the means for implementing the infrastructure should be provided basic services with only nominal costs.
- Leverage existing county investment in 800MHz trunking systems.
- Utilize the skills, resources, and leadership of county / city personnel in achieving statewide goals.
- Obtain technology which is APCO 25 compliant in order to reduce long term costs.
- Develop plans on a county by county basis optimizing each county's need for portable and in-building coverage with the state plan for mobile communications.
- Technology transparency - public safety officials should not have to be aware of the technology.
- Data functionality - access to the full CJIN Network.

Governance

The management structure required to support the statewide mobile voice and data network should have the following attributes:

- Heavy participation from communication officials who are experienced in system management in the counties, cities and local agencies
- Regional coordination for integrating local systems and engineering support
- Centralized administration and policy board

The key to success of the statewide voice and data network is the involvement from the communications professionals at the city and county level. These individuals are the most experienced at implementing, managing, and administrating trunked radio systems. They have been involved in organizing and managing statewide efforts, including NCRCPC and NCSUN. In recognition of this, a governance model is being proposed which ensures that local needs are heard while statewide strategies are being implemented. The governance model includes a Statewide Policy Board, Regional Operations Committees, and a Managing Organization. The following describes the role of each of these organizations.

Statewide Policy Board

The purpose of the policy board is to approve standards and strategy, and provide direction in regards to supporting user requirements and establishing priorities. The policy board should be representative of local and state agencies with significant requirements for mobile voice and data. In order to ensure that the main priority of the board is public safety, at least sixty percent of the members of the policy board should be directly involved in the public safety field. The

remaining forty percent should consist of significant participation from other major users. The policy board should include representation from the IRMC, the Controller's Office, CJIN Governance Board, and the Department's of Transportation and Emergency Management. The Statewide Policy Board should meet at least quarterly.

Regional Operations Committee

The purpose of the Regional Operations Committee is to provide input on a regional basis for management and operations of local and regional systems. The committee should consist of one representative from each county in the region. From the representatives, a chairman should be elected which will represent the Regional Operations Committee on the Statewide Policy Board. All users would be encouraged to attend the Regional Operations Committee proceedings in order to learn of new and ongoing activities and to promote their requirements. Six to eight regional operations committees should be established.

Managing Organization

The responsibility of the managing organization is to issue procurements, oversee daily administration, and report to the Mobile Voice and Data Statewide Policy Board and the CJIN Governance Board. The managing organization will be supplemented with financial and personnel resources required to fulfill the mission of statewide mobile voice and data. Included in its responsibility will be the function of providing regional system management and engineering support; managing contractors and equipment vendors; coordinating regional and statewide meetings; and carrying out the policies as approved by the Statewide Policy Board. The managing organization should have the following attributes:

- Be a large stakeholder in a statewide mobile voice and data
- Have experience in the implementation of statewide radio systems
- Demonstrate a willingness to support and an ability to understand a variety of user requirements
- Be willing to work with local agencies to support their initiatives

- Be capable and willing to work with all levels of government, including the Governor's Office and the General Assembly to build support for mobile voice and data systems
- Understand the dependencies of law enforcement and public safety of radio systems.

Based on these requirements, it is recommended that the State Highway Patrol perform this function. They currently maintain a statewide radio system which supports numerous agencies. They have already played a leadership role in directing attention to the need for statewide mobile voice and data. And they have also demonstrated a concern for supporting the needs of other agencies outside the criminal justice and public safety arena.

As the managing organization, the SHP will need the support of several other organizations during implementation. One key role will need to be played by SIPS in providing analysis and design support, as well as through the use of the NCIH and wide area networks, when appropriate. SIPS, should also be recognized as a leader in this initiative and should be relied on to continue to provide the support and leadership. However, SIPS is a receipts-based organization which must and should be remunerated for its continuous efforts.

County User Groups

Each county should organize a user group in order to identify requirements and implementation issues. The user groups should include county public safety and law enforcement.

Mobile Data Strategy

The strategy of the mobile data effort is to provide a variety of paths into the CJIN network from mobile data terminals. Pathways include CDPD, RAM, ARDIS as well as a statewide mobile data channels which are added onto the voice 800MHz infrastructure. In order to provide the access to the CJIN network for RAM, ARDIS, and CDPD access, only a simple leased line from these networks to the CJIN network is required. If a user or user group authorized to access the

CJIN network intends to use these vehicles, they would be responsible for packet costs and all vehicle costs while the state implements the leased line connection. Reasonable use must be shown before these lines are installed.

In order to provide a statewide mobile data network which is piggybacked on top of the state voice trunking system, a decision needs to be made as to whether the state should: 1) adhere to APCO 25 standards for data communications; 2) allocate additional channels dedicated to data; or 3) provide some combination of solutions. This decision should be made in concert with the technology which is available upon award of the contract. If APCO 25 compliance is all that is specified, additional channels may still have to be identified in order to enable large file transfers and to address data traffic congestion issues. In this area, the state needs to remain flexible in the near-term in order to enable themselves to take advantage of emerging technologies which will improve throughput and reduce band width requirements.

Guidelines for State / County Cost Sharing

From the onset of the project the counties made it clear that the state should not charge them for providing 800MHz trunking services. In fact, a representative from one county posed the question, "How much could they charge the state for allowing them to use their system?" Fear of the state imposing a receipts-based system for local agencies to use their own technology was echoed throughout the focus groups. Local public safety organizations have consistently demonstrated that they are willing to cooperate with each other and with the state. As demonstrated by the exchange of radios, the cooperative management and allocation of financial resources, and the numerous user groups and working committees which are in place now in North Carolina. This coordination and cooperation has been done in the interest of public safety, efficiency and effectiveness; with an attitude of "what's mine is yours"; and with a mutual respect which mitigates potential abuse. While the reasoning for a receipts-based system holds water in many situations, it is clear that in the case of public safety radio communications, it is a weak and self defeating argument.

This following proposes an alternative for how the state and counties / cities should share the cost of implementation of the statewide mobile voice and data system. This model was developed in collaboration with local and state communication officials. The objective of the model is to ensure local buy-in from large counties which already have extensive investments in 800MHz trunking technology while providing coverage in small counties without the means to

implement or support this technology. The salient features of this cost model are a) counties without requirements for extensive portable coverage will be provided with mobile coverage at no cost; b) counties with existing investments in 800MHz trunking technology will be provided upgrade assistance to comply with the statewide standards; and c) counties with no investment in 800MHZ technology will receive the equivalent cost supplement of the mobile coverage plus 25% of the cost of the portable coverage as identified during the county analysis.

- If the state's requirements for mobile communications are the same as the counties' requirements for portable communications (no additional sites are necessary), the state should fund the entire cost of the trunking system.

- If a county's requirements exceed the cost of the state's requirements for mobile communications, the county should pay for 75% of the additional cost of the trunking system with the state paying the remaining 25%.

- For cities /counties with current investments in 800MHz technology which is upgradable, the state should fund 50% of the upgrade costs. If the technology is not upgradable, the county falls under the previous guideline.

Based on these guidelines, using the previous cost model, costs would be allocated as follows:

Equipment	Unit Cost	Quantity	Subtotal	State	County/Agency
Trunked Repeater Stations	$20,000	3,400	$68,000,000	$42,500,000	$25,500,000
Conventional Repeater for Mutual Aid	$15,000	320	$4,800,000	$3,000,000	$1,800,000
Trunking Controller	$300,000	80	$24,000,000	$15,000,000	$9,000,000
System Manager	$180,000	80	$14,400,000		$14,400,000
Dispatch System Voice	$100,000	80	$8,000,000		$8,000,000
Digital/Analog Voting Comparator	$10,000	80	$800,000	$500,000	$300,000
Repeater Antenna Systems	$35,000	160	$5,600,000	$3,500,000	$2,100,000
Microwave Link Upgrade	$10,000,000	1	$10,000,000	$10,000,000	
Radio Towers	$400,000	35	$14,000,000	$8,750,000	$5,250,000
Equipment Building	$100,000	35	$3,500,000	$2,187,500	$1,312,500
Emergency Generator	$100,000	35	$3,500,000	$2,187,500	$1,312,500
Inter-Zone Overlay	$115,000,000	1	$115,000,000	$115,000,000	
Vehicle Radio	$3,500	25,000	$87,500,000		$87,500,000
Portable Radio	$3,000	50,000	$150,000,000		$150,000,000
Mobile Data System	$6,500	10,000	$65,000,000		$65,000,000
Data Switch	$2,000,000	1	$2,000,000	$2,000,000	
Data Controller	$125,000	4	$500,000	$500,000	
Total Equipment			*$576,600,000*	*$205,125,000*	*$371,475,000*
Technical Assistance @ 10% of Total			*$57,660,000*	*$36,037,500*	*$21,622,500*
Grand Total			**$634,260,000**	**$241,162,500**	**$393,097,500**

Ongoing Costs

The allocation of ongoing costs should reflect services received. Ongoing costs related to the roaming stock (vehicle mounted and portable radios) are the users responsibility. Ongoing costs related to the infrastructure, such as tower lease costs, leased line costs, and maintenance will be negotiated on a county by county basis. The key criteria will be to keep the accounting simple with the basic understanding that the taxpayer is paying for it independent of whether it is through state, local, or county budgets. Potential formulas could be based on number of subscriber units or number of subscribers. Fees should generally only cover administrative and actual costs and should not attempt to recover capital. For budgetary purposes, users have stated that they prefer fixed monthly costs rather than variable costs such as those offered by utilities.

One potential example of the state / county agreements are as follows: the state negotiates with a county with a large existing investment for free service for a specified number of subscribers for a limited period of time in exchange for an upgrade grant. Alternatively, for a state-run site in a small county, the state may charge some nominal fees for county subscribers to cover the administrative costs of adding users and maintenance of the leased lines and tower sites.

Allocation of Funds

Depending on the county, the state may elect to provide funding to the counties using a variety of mechanisms, including grants, joint purchase agreements or a partial ownership, or full ownership. The determining factors will include county participation, current investment, staff experience, and participatory attitude.

Implementation Tasks

The strategy for implementing the statewide mobile voice and data network is to:

- conduct a frequency identification study
- expand the MODAP pilot
- perform a county by county analysis of the voice and data requirements
- issue an RFP
- manage implementation

Frequency Identification Study

The purpose of the frequency identification study is to identify the channels which will be used across the state for mobile voice and data. This study could be incorporated into the county planning analysis, however, a shortage of, and competition for frequencies suggests that the study be completed before June of 1995. This effort must be initiated immediately in order to ensure that appropriate frequencies are available for implementation. In addition, this study should be done in coordination with the State Highway Patrol's current effort to license 96 transmitter sites throughout the state to support 800MHz mobile data.

Among the issues which should be addressed are:

- use of the NPSPAC frequencies
- review of the Region 31 Plan for efficiency and effectiveness in light of the CJIN effort
- refarming of existing usage in light of the introduction of statewide trunking technology

Expansion of the MODAP Pilot

The MODAP pilot successfully demonstrated the ability to provide information from the DCI, SIPS, and AOC systems to the mobile data terminals. This pilot effort was such a success that some law enforcement organizations invested in roaming stocks, other organizations complained about not being involved, and still others inquired how to participate. As a result of this effort, the state has obtained a wealth of experience in implementing mobile data systems which it should not allow to erode. Further, some local law enforcement organizations are concerned that their significant roaming stock investment will become ineffectual if the project is allowed to lapse.

In order to continue to build on the success of the MODAP pilot, the project should be expanded to include the following:

- Determine the impact of encryption on the performance of the system.
- Determine the impact of large files on the system, specifically Criminal Case History.
- Add additional users to determine the stress on the network.
- Test the use of NCIH or the state WAN as an integral part of the system.
- Expand geographic coverage to enable other law enforcement agencies to understand the technology and uses.

The following table suggests an annual budget for the expansion of the MODAP effort.

Budget for existing capability	$200,000
Addition of 100 MDTs $12,500/month*12	$150,000
Software security encryption	$50,000
Additional site equipment (DSU, Digital Transmitters)	$100,000
Total	**$500,000**

County Planning Study

Conduct a county-by-county analysis of user requirements. The county planning analysis will work with each county to determine county needs for portable and in-building coverage. Based on these needs, guidelines for budgeting and implementation will be produced which will assist the county in developing their radio infrastructure. In addition, an evaluation of existing and potential tower sites should be conducted. For counties with existing infrastructure, the infrastructure should be documented and a plan developed to upgrade existing systems to APCO 25 compliance.

Issue Implementation Contracts

Based on the county planning analysis, the state should issue an RFP for procurement of a statewide mobile voice and data system. This procurement should be structured such that counties / cities may buy into the procurement as they are available to budget and support the implementation of the 800MHz mobile voice and data systems. The procurement should be a multi-year indefinite quantity contract which will include purchase, lease, and lease to purchase alternatives that will enable counties to determine how they will obtain equipment. In addition, the contract should include the provision of engineering and support services to facilitate planning, maintenance, and engineering activities. A second services contract will also be necessary to provide vendor independent technical perspectives, quality control, and to fulfill administrative requirements. The state may elect to be involved directly in the purchase or lease of the equipment or may issue grants to counties and enable them to implement the entire systems. This decision should be made on a county by county basis considering the infrastructure, capability, and approach of each county.

Benefits to CJIN

The benefits to CJIN of a statewide mobile voice and data system include:

- Improved interagency communication - interoperability
- Reduced life-cycle costs
- Improved use of available radio spectrum
- Sharing of fixed radio communications resources
- Mobile and portable access to CJIN electronic information
- Enhanced officer safety

Statewide Survey Results
When law enforcement officials were asked in the statewide survey how useful 800MHz trunking technology would be for voice and data communications, over 87% of the respondents indicated that it would be useful. When asked how satisfied they were with their communications systems 35% of the 800MHz users responded very satisfied compared to 11% responding very satisfied for UHF and VHF radio users.

Best Practices - State of Michigan

In March 1994, Michigan awarded a not-to-exceed contract to Motorola for $187 million for a statewide 800MHz trunked radio system. The contract will be implemented in four phases over 10 years. The system will provide statewide roaming with 97% area coverage for mobile units. It is a turn-key contract which includes 181 towers, four to six base stations per tower, radio infrastructure equipment, microwave systems, control centers, and 3,000 subscriber units. It is intended for use by all state law enforcement and public safety agencies.

They charge each user a $250 initial fee and $300 per year thereafter.

The vendor has agreed to upgrade all equipment to APCO 25 standards.

No mobile data terminals, data equipment or channels are planned at this time until standards are evaluated. There are no simulcast systems planned in order to conserve frequency. Because of the age of the towers and the fact that they did not meet current safety standards, none of the existing towers were used.

Implementation times:

1985 through 1989 - several studies were conducted recommending use of 800MHz trunked systems
October 1992 - RFP was disseminated
May 1993 - three question and answer periods were completed and bids were received from Motorola and Harris Corporation
September 1993 - both bids were determined unacceptable and were rejected
November 1993 - BAFO bids were received
March 1994 - Harris bid was determined to be non-compliant and Motorola was awarded the contract
December 1996 - acceptance of phase one

There are significant lessons to be learned from the request for proposal and the evaluation methodology utilized in this effort.

Best Practices Survey - Groton Connecticut
Law enforcement and public safety agencies have installed computers into the vehicles equipped to send data over Bell Atlantic Mobile Systems (BAMS), Inc CDPD network. This site is believed to be the first law enforcement application to use CDPD. CDPD claims to provide 19.2Kbps transfer rate and they are reporting three second response time. They are using Software Corporation of America (SCA) software, and Telepad, Inc. pen-based computers. They have negotiated a fixed cost of $100 per month per vehicle for CDPD usage.

Best Practices Survey - Dade County, Florida
Dade County has implemented a forty channel, seven site system (six sites are simulcast) using Ericsson analog and digital technology. It will support all county efforts, including public safety, law enforcement, and public works. The total cost of the system, including initial subscriber units is $39 million. They expect to eventually support up to 11,000 users, including 2,500 law enforcement officials. Initially they have no data capability though they are pursuing initiatives in this arena. Initial investigations have led them towards non-ruggedized laptops rather than ruggedized computers or mobile data terminals for end-user devices. They recommended bringing public works onto the system first to pilot test the applications. In this way, law enforcement and public safety will not be ill affected by early technical glitches. The contract was awarded two years ago. When it was awarded, Ericsson had promised APCO 25 compliance. Ericsson is currently backpedaling on this issue. They use the NPSPAC 800MHz conventional mutual aid channels to talk with the highway patrol and other agencies.

Risks

Digital Radio is not the same technology as digital telephone. The digital telephone is system architecture which is based upon quantizing the voice and then regenerating the information. The only loss in the conversation is the one time quantizing loss. Digital radio system architecture is based upon comparing the audio to some simulation and then

sending down the communication channel the address of the information simulation. At the receiving end, the voice is regenerated, not reconstructed. This process is referred as the *vocoder*. The hardware for the APCO 25 vocoder to date has not been shipped or evaluated by the user community which presents a significant risk if implementation is predicated solely on the APCO 25 standards. To mitigate this risk, the user community will need to evaluate the effectiveness and usability of the digital technology prior to award of procurements. Some early products were rumored to provide unsatisfactory voice quality. However, upon questioning of individuals intimately involved with the APCO project, they felt strong that these concerns have been addressed with newer products.

Vendor Contacts

Altell Mobile Data (CDPD)	Rick Warco
ARDIS	Larry Chay
Ericsson	Jim Amos
Motorola	Curtis Baker
RAM Mobile Data	Charles Machinshky
Software Corporation of America (SCA)	Thomas Doyle

STATEWIDE AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

NEED FOR CHANGE

In most parts of the state of North Carolina the positive identification of offenders can take up to ten days to two weeks into the offender's journey through the criminal justice process. It is possible that the offender will see a magistrate, be booked into jail and / or released on bond, be charged by the district attorney, meet with a public defender, and be through a first appearance in district court before being identified as a person with a previous criminal record.

RECOMMENDED SOLUTION

Establishment of a statewide automated fingerprint identification system (SAFIS) which supports the following goals:

- SAFIS will provide to user positive identification based on fingerprints, in less than two hours.
- SAFIS will facilitate the universal usage of the State Identification (SID) number.
- SAFIS will trigger rapid identification of an individual's past and current involvement with the criminal justice system.

SAFIS will consist of the following components:

- Universal usage of a single, statewide, personal identifier based on fingerprints to link an individual offender's record of arrests, court cases, dispositions, custody, and release data.
- A centralized arrest intake facility in each county with a livescan device that is electronically linked to the State Bureau of Investigation's (SBI) Division of Criminal Information (DCI) to record fingerprints of all felons and misdemeanants.
- A centralized automated identification center at the SBI that operates 24 hours per day, 7 days per week.

Need for Change

In most parts of the state of North Carolina the positive identification of offenders does not happen in a reasonable amount of time. Because the state does not allow pretrial detention, offenders who are arrested must be taken before a magistrate for an initial appearance, without unnecessary delay, for determination of conditions of pretrial release. It is common practice throughout the state to wait to fingerprint offenders until after they have seen the magistrate. Thus, it is not uncommon for offenders to progress through the criminal justice system using aliases, and to benefit from decisions that are made based on incomplete knowledge of criminal history.

In-state survey results indicate that 97 percent of law enforcement respondents rated positive fingerprint identification as extremely important or important.

When an individual is incorrectly identified the following lapses in information can take place:

- **Law enforcement officers** do not know if they are dealing with an individual who has a criminal history, has outstanding warrants, is violating probation or parole, or is known to be dangerous.

- **Magistrates** do not know if the individual has a record of failures to appear, bond forfeitures, outstanding orders for court, or is a probation or parole violator.

- **Jailers** do not know if the individual has a history of violence or escapes.

- **Prosecutors and defense attorneys** do not know whether the individual has a prior criminal history and convictions.

- **Judges** do not know the person's criminal history and past court dispositions, necessary for structured sentencing.

- **Probation and parole officers** are not notified if an offender has violated conditions of probation or parole.

Under the current system, fingerprint cards are mailed to the SBI / DCI for identification. By the time offenders are properly identified, a process that normally takes ten days to two weeks, key decisions have been made about their arrest, custody status, charges, and case. When offenders use false names or demographics, to avoid their past criminal history, a window of opportunity is opened that allows them to be inappropriately released. The offender may be released without being charged, be charged but allowed to post inappropriate bail, or be improperly charged or sentenced. The result is that due to the length of time it takes to positively identify an individual, the criminal justice system is allowing criminals to avoid responsibility for their actions.

Identification Numbers

The SBI assigns each fingerprinted offender an individual, State Identification (SID) number. Currently, this number is based on fingerprint identification. When the SBI assigns the SID number, it transmits the number to the arresting agency. This information comes to the local agency approximately ten days to two weeks after the time it would be most useful.

Many local agencies never populate their databases or files with the SID number because it would require an additional data entry step, and it is assigned too late to be of practical use to them. Instead, they assign and use Local Identification (LID) numbers. These local numbers are unique to each county and city that issues them. Offenders who are arrested on certain charges also receive a Federal Bureau of Investigation (FBI) number. This number is transmitted from the FBI to the SBI computer, which in turn transmits it to the arresting agency.

Offenders who are sentenced to state prison receive Department of Correction (DOC) numbers. DOC also uses the FBI number. There is currently a project to consider populating the Offender Population Unified System (OPUS) database with SID numbers. Offenders who receive active sentences are fingerprinted and assigned an SID number; those who are on felony probation are fingerprinted; however, those who receive inactive sentences and commit less than a serious misdemeanor offense are not fingerprinted and do not have SID numbers assigned to them.

Each offender has multiple identification numbers throughout the criminal justice system, and a unique, common number is never established or cross-referenced between local, state, and federal files. Consequently, there is no method to connect a person's criminal history by a single number. Moreover, the criminal history is fragmented between local, state, and federal databases.

Fingerprint Process

In North Carolina, it is mandated by statute that all individuals charged with a felony must be fingerprinted. With exceptions, individuals charged with misdemeanors may be fingerprinted, when booked into jail. An administrative order

by each of the senior resident superior court judges directs which individuals charged with misdemeanors must be fingerprinted within each judicial district. In many counties, the fingerprint process is considered a recordkeeping requirement of the state and federal governments and, therefore, sometimes may not be done. Fingerprinting is generally done after the offender has seen a magistrate. If the magistrate releases the offender because of lack of probable cause, then that offender may not be fingerprinted at all.

All law enforcement agencies forward their fingerprint cards to the SBI, which then forwards first time felony and serious misdemeanant offenders' cards to the FBI. Typically, offenders are fingerprinted in one of two ways:

- Offender's fingers are manually inked, and impressions are rolled onto a ten-print card. Two full sets of prints must be rolled, one for the SBI and one for the FBI. (Often a third set of prints is rolled for the local agency's own use.) The SBI also requires palmprints. Demographic information is typed or written on the fingerprint cards and on a Final Disposition Report Form, which is forwarded to the clerk of the superior court by the magistrate.[1] The SBI and FBI fingerprint cards are sent to the SBI via the U.S. Postal Service or the State Courier Service.

[1]The fingerprint card and the Final Disposition Report establish the link between the SBI and AOC databases with the population of the unique check digit number on the AOC database and with the population of the court case number on the SBI / CCH databases.

Current Fingerprint Identification Process — takes up to 2 weeks

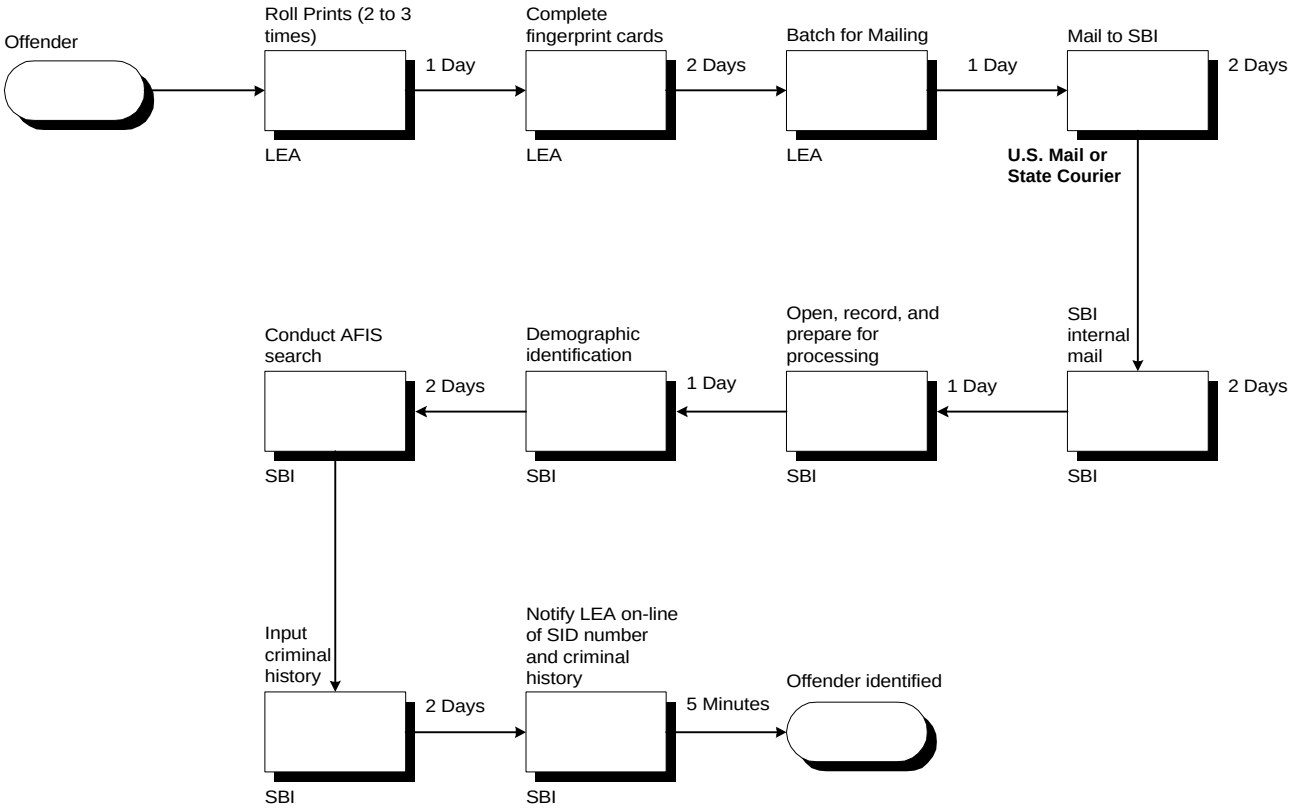


Figure VI.6-1

- Offender's fingerprints are scanned into a livescan device. Demographic information is either passed to the

livescan system or input manually, and the fingerprint cards are printed. Alternatively, the fingerprint card is printed and then demographic information is manually added to the card. A Final Disposition Report Form must also be completed. The Final Disposition Report Form is sent to the clerk by the magistrate. The SBI and FBI fingerprint cards are sent to the SBI via the U.S. Postal Service or the State Courier Service.

The inked fingerprinting process is time consuming and repetitive. It takes trained and experienced personnel to obtain good quality prints, and they must complete multiple copies of fingerprint cards for both the SBI and the FBI, and sometimes for the local agency also. A poor quality print requires that a new fingerprint impression be made. Approximately 10 percent of the fingerprint cards submitted to the SBI are rejected due to incomplete or inaccurate information.

When SBI receives a fingerprint card, first it conducts a name check on the card. If there is a "hit" with similar demographic data, the technician manually pulls the fingerprint card on file, and compares the incoming card with the card on file. If the technician identifies the fingerprint cards, a second technician reviews the cards to verify the match. If the fingerprints do not match then the technician runs a search on the AFIS system. For the sixty to sixty-five percent who are repeat offenders, ninety percent of these fingerprint cards are identified by the name search.

On average, SBI staff runs 300 AFIS searches a day. These searches are now done in overnight batches, and staff reinput the same information into various computer systems at least three times on every fingerprint card it processes. It takes approximately two weeks for a fingerprint card to move through the entire identification process, from booking in jail to receipt of a criminal history response from the SBI. If the individual is a first time felon, SBI forwards the designated packet to the FBI, which operates a national, centralized repository, and clearinghouse for fingerprint records of felons and serious misdemeanants. This clearinghouse acts as a locator or index of criminal arrest activity throughout the United States.

Offenders who are received by, or released from, the DOC are fingerprinted for purposes of identification at acceptance and release. The DOC submits the fingerprint cards to the SBI for all inmates who are serving an active sentence in state prison. Because of the volume of misdemeanants, for many of these offenders the SBI does not have arrest records on file. These fingerprint cards are processed by the SBI in the same way as the cards received from law enforcement

agencies. There is a quality control issue regarding the demographic information recorded on the fingerprint cards. The cards are handed-off between numerous units within the DOC and often they are difficult to read because there are many handwritten additions, deletions, and changes. When this information is unreadable, contradictory, or invalid, the cards are rejected by the SBI.

National Trends

The FBI is in the process of developing standards for an Integrated Automated Fingerprint System (IAFIS), which will transform the FBI's ability to maintain a current and effective fingerprint identification operation that interfaces with the entire nation. This effort is being led by the FBI's National Crime Information Center (NCIC) Advisory Policy Board. The goals of IAFIS include the following:

- Simpler and faster service interface for federal, state, and local users
- More complete and accurate criminal history record for national checks
- Targeted start-up date in 1996

North Carolina was the second state to implement the National Fingerprint File (NFF) with the FBI. This in an effort to reduce redundant data at the federal and state level. The state is responsible for maintaining arrest, court, and custody criminal history data. The FBI no longer maintains a copy of the data in its files. In addition, the state only submits fingerprint cards to the FBI for first offenses. Subsequent offenses are processed by the SBI and entered into the state criminal history system, but not forwarded to the FBI. Nonetheless, local law enforcement agencies are still required to complete duplicate fingerprint cards and Final Disposition Report Forms for known felons and some serious misdemeanants, though the FBI portion of the package is no longer used due to SBI's NFF participation.

Recommended Solution

- Usage of the SID number by law enforcement, courts, and corrections.

- Establishment of centralized, county intake facilities, which operate twenty-four hours per day, seven days per week.
- Establishment of a statewide, centralized AFIS center, which operates twenty-four hours per day, seven days per week, and is located within the SBI.
- Coordination and integration between Mecklenburg County's AFIS database and the SAFIS system.
- Positive identification of all felons and misdemeanants within two hours of arrest, ideally in thirty minutes.[2]
- Coordination with IAFIS standards and guidelines.

We recommend that the state develop a computerized, identification system based on SID and fingerprint records for all offenders arrested on felony and misdemeanor charges. Individual counties, using livescan devices, will electronically forward fingerprints to a centralized processing center, located at the SBI, that will process fingerprints 7 days a week, 24 hours a day. All state and local agencies should adopt the same process and procedures. Mecklenburg County, which already runs a 24 hour / 7 day centralized intake facility, should be electronically connected to the SAFIS system. Counties are already in the process of procuring livescan devices and AFIS equipment, and developing systems that are independent and not integrated. It is imperative that the CJIN governing body takes the lead in setting technology and operational standards for a statewide automated fingerprint identification system.

State Identification Number

The state should encourage the universal usage of SID numbers, based on fingerprints, to link an individual offender's record of arrests, court cases, dispositions, custody and release data. So that the state identification number positively and uniquely identifies offenders throughout the criminal justice system, it will be necessary to fingerprint all offenders

[2] The two hour limit corresponds with NCIC 2000 standards.

charged with felony and misdemeanor offenses.[3] In addition, we recommend that juvenile offenders be fingerprinted and assigned a SID number. Please see Section VI.12, Juvenile Records Automation for more recommendations.

A change to the state's current practice of fingerprinting no misdemeanants or only serious misdemeanants, as opposed to all misdemeanants, will require an administrative order by the senior resident superior court judges or a change in state law.[4] If all felons and misdemeanants are fingerprinted there will be a more comprehensive usage of the check digit number to link SBI and AOC records. This will result in more accurate information exchanges between the two agencies. In addition, the universal usage of the SID number will facilitate the consolidation of offender records and encourage the elimination of duplicate identification numbering systems across the state. If the SID number is not propagated widely, then there will only be incremental improvements in identifying the state's criminal population quickly and efficiently.

We are aware of the fact that the IRMC is currently discussing the institution of a statewide, unique identifier for all North Carolina residents. In addition, state agencies, such as the Division of Motor Vehicles and Department of Human Resources, have discussed fingerprinting for identification purposes the populations they serve. There may be future potential to link these numbers with SID number.

Centralized Intake Facilities

[3] We recommend the use of fingerprints to establish positive identification because at this time it is the most accurate and widely accepted method. The identification system used by CJIN should be flexible enough to adopt other identification methods, such as DNA, with advances in science and technology.

[4] N.C.G.S. 15A-502.a "A person charged with the commission of a felony or a misdemeanor may be photographed and his fingerprints may be taken for law-enforcement records only when he has been: (1) Arrested or committed to a detention facility, or (2) Committed to imprisonment upon conviction of a crime, or (3) Convicted of a felony. This section does not authorize the taking of photographs or fingerprints when the offense charged is a class 2 or 3 misdemeanor under Chapter 20 of the General Statutes, 'Motor Vehicles.'"

Each county should implement a centrally located, centralized arrest intake facility and record the fingerprints of all felons and misdemeanants with a livescan device. A centralized facility will take advantages of economies of scale and reduce the number of necessary livescan devices. Fingerprint images and demographic data should be transmitted electronically to the SBI, 24 hours per day, seven days per week.

Recording fingerprints with a livescan device is more efficient than rolling prints with ink, and higher average quality fingerprint impressions are produced. Prints only need to be scanned once, and data input once, rather than the multiple steps required for manually producing fingerprint cards and forms. Moreover, automatic data entry edits and validations will prevent technicians from omitting information or entering invalid data, such as a date of birth in the seventeenth century. In addition, the technician can review the prints online and if they are of poor quality, can re-scan them immediately, thereby building quality in at the front of the process, and reducing the number of rejected fingerprints by the SBI or FBI.

Fingerprinting all misdemeanants, as opposed to the current practice of fingerprinting only some of the serious misdemeanants and all felons, will increase each county's fingerprinting workload by approximately five times. The time saved by using a livescan device should help compensate for this increase. There will be opposition from some law enforcement agencies, specifically municipal police departments, which may consider it inconvenient to transport offenders to a centralized intake facility. Moreover, some counties may not have the appropriate facilities or staff resources to handle the workload associated with a centralized intake center and comprehensive fingerprinting of all felons and misdemeanants.

When positive identification is made by the SBI, law enforcement agencies will makes appropriate decisions about offenders based on correct information. Local agencies will use SID numbers as a unique identifier for each offender. [5,6] Local law enforcement could still use originating case agency numbers or incident numbers to track cases. Or, if all

[5] The North Carolina Automated Exchange of Criminal Justice Data Project (AECJDP) recommended that local agencies use SID numbers.

[6] The standardization of information and the establishment of an "event tracking number" are key steps in facilitating communication between criminal justice agencies (see Data Sharing Standards Development, Section VI.1 of this study).

felons and misdemeanants are fingerprinted, the fingerprint card check digit number could be used as the unique event tracking number on both the state and local levels. There will no longer be a need for local agencies to use LID numbers if all offenders who are arrested on felony and misdemeanor charges are fingerprinted, positively identified, and assigned a SID number.

Future Fingerprint Identification Process — will take 20 minutes to 2 hours

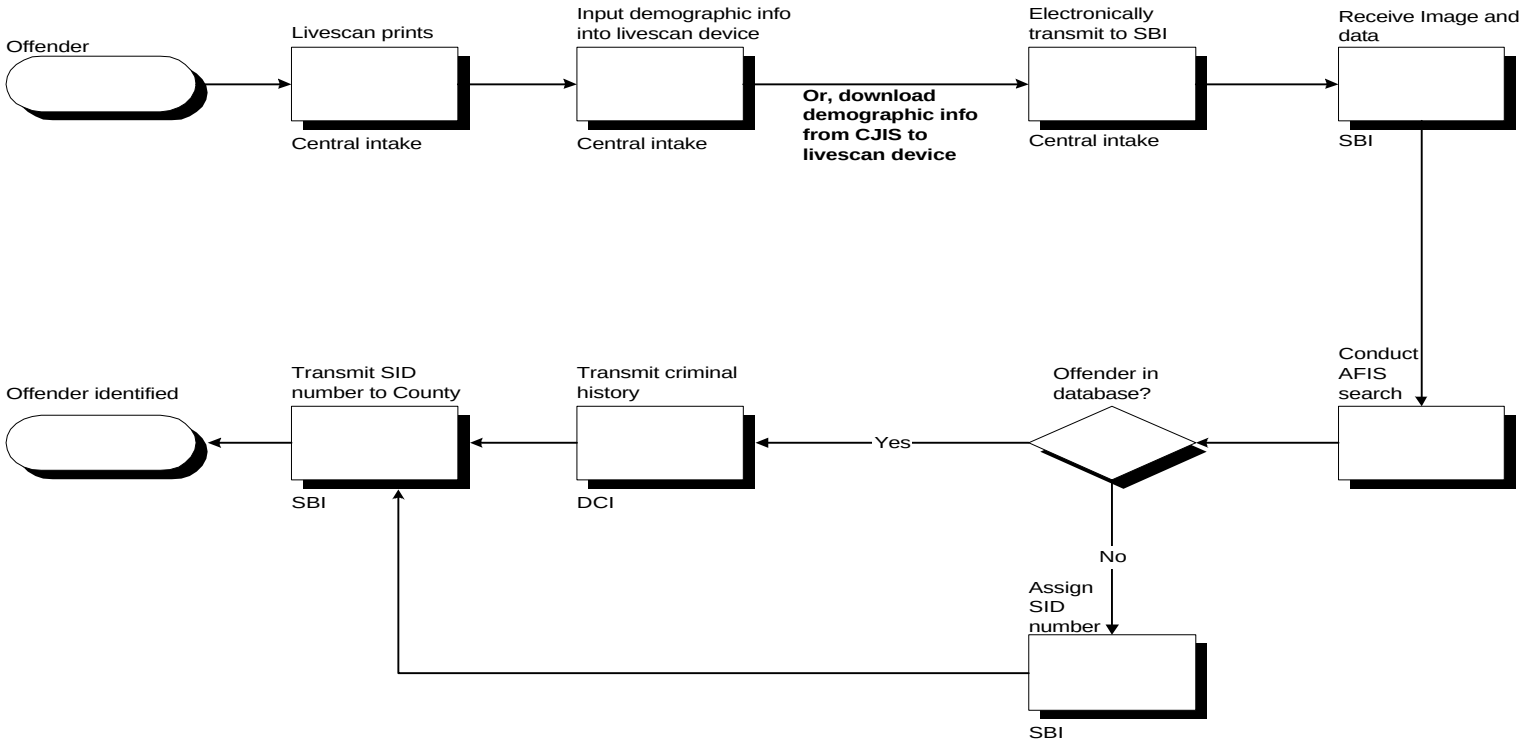


Figure VI.6-2

Centralized AFIS Center

Staff at the SBI should use AFIS technology to conduct the identification process 24 hours per day, 7 days per week. AFIS automatically extracts and digitizes identifying characteristics to enable the computer searching and matching algorithms to distinguish a single fingerprint from thousands of file prints that have already been scanned and stored in digital form. A computer-generated image of both the incoming search print and the retrieved candidate prints are displayed side-by-side on the AFIS operator's computer screen. The operator visually verifies the match.

A match indicates the offender has a criminal record. When a criminal match is made, the SBI's Computerized Criminal History (CCH) will be updated automatically with the data accompanying the fingerprint image.

If the offender has no previous arrests, the SBI electronically assigns a SID number and notifies the local agency of the number. If a positive identification is made, the SBI notifies the local agency of the offender's criminal history and existing SID. Currently, staff at the SBI must input all information on the individual into the CCH database. Using livescan and electronic transfer of data, this data input step will be eliminated for SBI staff.

A number of counties have already purchased their own AFIS systems.[7] Most of these counties are using their AFIS systems to conduct remote searches of the SBI database against latent fingerprints for investigative purposes when there are no known suspects. Comparisons can be made between crime scene fingerprints and fingerprints in the database from previous arrests. These counties should continue to utilize their AFIS systems for this purpose.

Mecklenburg County has implemented a centralized intake facility and a countywide AFIS that do real-time searches against the county's own fingerprint database. Currently there is no interface between SBI's and Mecklenburg County's fingerprint databases at least in part because of proprietary architecture differences. We recommend that a technical solution be devised that allows Mecklenburg County to electronically transmit fingerprint images and demographic data

[7] Wake, Cumberland, and Mecklenburg counties each have one AFIS, Gaston County has two AFIS's, and the Rocky Mount Police Department operates a regional AFIS for eight counties in northeastern North Carolina.

to the SBI. Utilizing the regional concept, Mecklenburg County should continue to search its county database. The electronic transmission to the SBI would allow for simultaneous searches of the SBI's database, and with the implementation of IAFIS the FBI's database. It will automatically update the SBI's CCH. In addition, this would allow Mecklenburg County to receive the assignment of an offender's SID number.

DOC is also in the process of implementing livescan and remote AFIS technology. This will greatly improve its fingerprinting process and benefit the SBI because DOC staff access and update SBI information directly. Use of this technology will expedite offender identification within DOC, enhance criminal history records access time, improve consistency in offender records management, and eliminate duplication of data entry for records maintained at both the SBI and DOC.[8]

Implications of fingerprinting all offenders

Provisions must be made for those offenders who are charged but are never fingerprinted. If an individual is scheduled for court and has never been fingerprinted, there will be no SID number for this record. The AOC is presently installing warning flags on court calendars to identify individuals charged with felony offenses who have not been fingerprinted, and this could be expanded to include misdemeanant offenses. There should be a process to send the offender to the nearest livescan processing center. The offender can then be positively identified and be issued a SID number. This will fill a current gap in state and local recordkeeping.

If all misdemeanants are fingerprinted, the number of expungement orders may rise. Conversely, the abuses that occur in the current expungement process may be curbed because a positive identification and record check on a statewide basis can be made on the applicant before any orders are issued.[9]

[8] From DOC's grant application to the Governor's Crime Commission.

[9] Issues regarding expungements can be found in Volume 2, Focus Group Number 14.

Benefits

Benefits to the Criminal Justice System

- Improved information will result in better decisions made by all participants in the criminal justice community.

- The SID number will provide the foundation for an integrated and automated Statewide Identification Index. By positively identifying offenders in the criminal justice system through fingerprinting, the Statewide Identification Index will be more accurate than if it were based on demographic information alone.

- Positive identification will be made from the time an offender enters the criminal justice process.

- Increased accuracy, reliability, and timeliness of the CCH.

Benefits to the Division of Criminal Information

- Elimination of redundant data entry.
- Increased accuracy, reliability, and timeliness of the CCH.
- Ability to print as many fingerprint cards as needed from the electronic file from livescan fingerprint systems.
- Enhanced tracking capability of offenders who commit crimes across the state.
- Statewide standards for doing business.

Benefits to law enforcement agencies

- Increased identification accuracy and completeness of criminal history information.

- Reduction of redundant data entry. There will be no reason to manually fill-out duplicate fingerprint card information, this can be input directly into the livescan. If the county is automated, then the arrest information that has already been input into their own automated system can be downloaded to the livescan device.

- Reduced response time through the elimination of the bottlenecks created by sending fingerprint cards to the SBI through the U.S. Postal Service or the State Courier Service and eliminating the manual preparation steps to process fingerprint cards.

- Increased security during the process of fingerprinting due to immediate electronic transfer of images and data to the SBI. The risk of mixing up offenders' cards is eliminated, especially when processing inmates.

Benefits to the courts

- Positive identification of repeat offenders and completeness of criminal history information for determination of aggregate conditions of pretrial release.

- Judges will have proper information to determine sentencing requirements as required under structured sentencing guidelines.

Benefits to the public

- Positive identification of criminals at the time of arrest will protect past and future victims by not allowing offenders unwarranted freedom.

- Increased credibility in North Carolina's criminal justice system. If the public knew that the routine practice is not to identify offenders until "after the fact," and one dangerous criminal was released and then committed a violent crime, there would be significant negative publicity.

- Avoidance of false positives. Law enforcement officers reported numerous examples of offenders using an innocent person's identity, being charged with a criminal offense under the innocent person's name, and when the offender fails to appear, the innocent person is arrested. This can be avoided if all offenders are fingerprinted and identified at arrest. With first time offenders, AFIS cannot detect the use of innocent persons' identification at arrest time; however, innocent persons will have a means to later clear their names.

- A comprehensive database for governmental and private employers who require fingerprint-based criminal history checks, such as day care centers, schools and hospitals, to search as part of the employment or licensing processes.

Recommended Technology

Livescan

A livescan system is an electronic device that utilizes image scanning technology to capture digitized fingerprint images. An offender's fingers are rolled onto a scanner attached to the livescan device and the device captures an image of the fingerprints. With a print server, fingerprint cards can be printed if needed. The livescan operator can evaluate the quality of the fingerprint impressions on line, and re-roll the fingerprints if necessary.

A complete set of ten uncompressed fingerprint images contain 2.5 to 3.0 megabytes of data. Transmission of this data requires a network with sufficient bandwidth so that throughput is not hindered at peak times. It is important to note that the FBI for IAFIS is in the process of approving a compression scheme that will compress these files by a factor of fifteen. However, the state, under the auspices of the IRMC, has developed compression standards for the North Carolina Information Highway (NCIH). The federal and state standards are different and CJIN will need to decide on the compression method it will use. This decision will greatly impact efficient storage and transmission of fingerprint images and data. If throughput to the SBI is a factor of six, but compression is allowed by a factor of fifteen, then additional bandwidth and central AFIS processing power and storage space is necessary only for potential increases in future workload.

We recommend a method that transmits fingerprint images and data directly into the SBI's AFIS. All local systems will need to interface with the state in a compatible mode, using TCP / IP standard protocols. In order to receive images and data, the SBI will need a connection and remote gateway that will accept the increased volume of files and data. It will also need software to process the incoming workflow. For first time felony offenders it will still be necessary for the SBI to have a print server to print out a copy of the prints and data to send to the FBI.[10] Otherwise, images and data can be kept in the system.

There should be an effort to ensure that each county has at least one livescan device. Each county should decide the appropriate location to house its livescan device. There are already many counties that have requested grants to purchase livescan equipment, and that have already issued Request for Proposals (RFPs) to vendors who supply livescan equipment. In order to ensure connectivity and compatibility with SAFIS and IAFIS, livescan equipment must comply with standard data format, transmission and compression specifications. We recommend that counties comply with the livescan requirements developed by the SBI.

Automated Fingerprint Identification System

AFIS technology reduces an individual's fingerprint image into minutiae based binary code. This code can be searched against the binary minutiae code of all of the other individuals contained in a database. An AFIS scan searches an offender's fingerprints against previously recorded fingerprints in the state's database. AFIS can match individual fingerprints at 1,600 matches a second. Disk access lengthens search time. To speed up search time, AFIS can limit searches by using demographic-based filters, however, filters introduce the possibility of false negatives. On the other hand, filters can also increase accuracy by reducing the number of respondents for an individual to look at.

The SBI will need sufficient technology to store and forward the fingerprint images and data it receives. The telecommunications network must not only have the capacity to receive a high volume of files and data from within the

[10] The FBI will soon be able to receive fingerprint images and data electronically through its Electronic Fingerprint Image Print System (EFIPS) program.

state, but it must also be able to transmit files and data between the national IAFIS, other out-of-state AFIS, and other in-state AFIS systems.

Initial Cost Factors

Cost Component	Cost ($)
Hardware[A]	19,000,000
Software Development[11]	1,000,000
Business Process Analysis[12]	792,000
Project Management[13]	1,584,000
Total	**$22,376,000**

[11] Software development consists of integrating SAFIS with local CJIS systems.

[12] Business Process Analysis requires 3 full time equivalents (FTEs) for 12 months. All FTEs are costed @ $22,000 per month.

[13] 2 FTEs for 3 years.

Ongoing Cost Factors

Cost Component	Annual Cost ($)
Maintenance[14]	2,050,000
Training[15]	528,000
Total	$2,578,000

[14] Maintenance is estimated at 10% of the initial hardware cost and 15% of the initial software development costs.

[15] Ongoing training requires two full-time staff.

A. Hardware Costs

Cost Component	Quantity	Cost ($ per unit)	Total ($)
Statewide AFIS[16]		10,000,000	10,000,000
• CPU[17]			
• AFIS Terminals			
• Optical Server[18]			
• Database Server[19]			
Livescan Stations[20]	100	90,000	9,000,000
		Total Cost	**$19,000,000**

[16] Based on discussions with SBI with regard to current procurement proceedings.

[17] The statewide AFIS system comprises these four components.

[18] Optical server storage requirements: 2.5 to 3.0 megabytes / person
1 million person database
≈ 3 terabytes @ 1 terabyte / server
≈ 3 servers

[19] 10 database servers are necessary to meet performance requirements and the possibility of future parallel processing.

[20] Station includes livescan device, laser printers with card handlers, and communication software to integrate with the Statewide AFIS system.

Cost Savings

- Reduce fingerprinting time and workload by using livescan device to scan fingerprints once, and input demographic data once, or download information from local CJIS.
- Reduce workload through elimination of redundant data entry and manual preparation processes.
- Eliminate expungements now necessary due to false identifications.

Quality Assurance

- Quality will be built in from the beginning of the identification process by using livescan. The livescan device will provide data edits and validations and the operator can review scanned prints and re-roll the prints if they are not usable.

- Verification is the key quality issue, and what causes the most harm. The model is for two persons to verify each set of prints. This will impact the SBI's staffing needs.

STATEWIDE MAGISTRATE SYSTEM

CURRENT SITUATION

In North Carolina, as few as six counties have automated or begun automating the magistrate process. The remaining 94 counties continue to handwrite or type processes, including arrest warrants and orders for release. This manual process requires the magistrate to spend time writing or typing on preprinted forms, not only original offender information, but also the same standard language each time an offender is processed. Demographic and other critical information manually entered by the magistrate is then re-entered by the Clerk of the Superior Court into the AOC's Court Information System (CIS), Criminal Module.

NEED FOR CHANGE

- The lack of automation in magistrates' offices creates a need for duplicate data entry by the magistrates, law enforcement officers, district attorneys, and clerks. This is a waste of the most valuable human resource to an organization - time.

- There is an inherent time delay between a magistrate's process and the clerk's ability to enter the information. As a result, law enforcement officers, district attorneys, and judges do not have the most up-to-date information and may make decisions about an individual without knowing about a "fresh" arrest or bond situation.

RECOMMENDED SOLUTIONS

- Implement an automated magistrate system for those counties that do not currently have one.
- Implement an interface between the proposed AOC magistrate system and SBI /DCI warrant system

Current Situation

Magistrate information systems across the state have evolved slowly and suffer from a lack of resources and uniformity. As few as six counties have automated or begun automating the magistrate process. The remaining 94 counties continue to handwrite or type processes, including arrest warrants and orders for release. Demographic and other critical information such as witnesses, is manually entered by the magistrate and then reentered by the clerk into the AOC's CIS. Additionally, in some counties arrest warrant information is reentered into a DCI terminal (if available) by the law enforcement agency. Buncombe and Mecklenburg are two of the counties that have been quite successful in implementing automated magistrate systems.

Even those counties with automated systems do not currently have linkage to the CIS system and, therefore, cannot automatically feed warrant information into CIS nor can the courts feed disposition information back to the magistrate system for updating. Because of the differences in the volume of processes issued and the levels of personnel support, information up-dating varies significantly from county to county. Therefore, information can not be relied upon to be current.

This latter issue is being addressed through the AOC's Local Interface Project (ALI). Currently three counties are participating in the development of a two-way feed that allows the transfer of information back and forth between

automated magistrate systems and the AOC's CIS system. However, this interface will not initially provide real-time access to information because of system limitations and batching requirements.

Need for Change

The manual entry of data, duplication of effort, and time delays inherent in the current magistrate process create a significant need for change. The system is currently very cost inefficient because personnel time is unnecessarily wasted. For example:

- To hand write or type information is more time consuming than using a word processor.
- Redundant, "boilerplate" information is currently recorded manually for each offender processed. This could be easily automated and printed directly on a process, eliminating the time required for manual entry entirely.
- Duplicate data entry by the magistrate and clerk could be eliminated by providing the magistrate with a system that allows for information entry directly into the CIS system.
- Duplicate data entry of arrest warrant information by the magistrate and a law enforcement agency can be eliminated by providing the magistrate automated system with a direct link to the local law enforcement system and/or the SBI/DCI warrant system.
- Manual searches for information and data editing can be automated. For example, outstanding warrants can be integrated into the automated system and electronically retrieved.

In-state survey results indicated that 89% of all respondents rated the ability to enter magistrate data electronically at the time of occurrence as extremely important or important.

The magistrate collects the most up-to-date information about enforcement actions resulting in arrests county wide. This information is necessary for law enforcement officers, district attorneys, probation / parole officers and judges in order to know which individuals have outstanding warrants, have been arrested, and/or have posted bond. The time delay created by the clerk rekeying this information creates a lag between the event and its inclusion onto the AOC's CIS system, making this information much less valuable.

Up-to-date warrant and bond information is important in day-to-day decision making. For example,

- law enforcement officers may have contact with an individual who is in violation of the terms and conditions of bond. However, if the information is not recorded and captured into the system real time, the officer may not have the information needed to identify it as an arrest situation. In fact, the offender may be in the process of absconding and will be successful because of system delays.

- law enforcement officers may arrest an individual out on bond for a new offense in a different county. The bonded offense may not be entered into the automated system yet. The offender is brought before a different magistrate and decisions about proper charges and bond are made without the most recent arrest information. Absent accurate and current information, the offender may be treated more leniently than the situation requires.

- District Attorneys will not have complete information about an offender and, therefore, may make inappropriate prosecuting decisions.

- an offender may be sentenced by a judge who has no knowledge of recent repeat offenses.

An automated magistrate system with a direct link to the AOC’s CIS system could provide real-time information to all of the criminal justice professionals who need the information to effectively make decisions about individuals who they deal with on a daily basis.

Approach

Implement an automated magistrate system for those counties that do not currently have one

Attention to both hardware and software needs will be necessary for most of the counties. This can be accomplished using a three step approach.

1. Identify standards and features for an automated magistrate system

The AOC should coordinate a statewide effort to develop standards relating to the automated magistrate system. Standardization in format and technology will provide some level of consistency and allow system upgrades to be easily enacted. Standard system features should be considered, such as the automatic:

- immediate appearance of easily readable demographic information to assist with offender identification.
- linking of all information about an offender to a Statewide Identification Index or number inquiry.
- presentation of all outstanding processes.
- presentation of predetermined screens for the magistrate to easily enter data. For example, the screens should be designed so that information:
  - is requested in the most logical sequence.
  - only has to be entered if it is unique to each offender.
  - phrased as "boilerplate" language will appear and print automatically.
  - that is required in a field must be entered before the user is allowed to advance to the next field.

Counties may wish to enhance their systems beyond the suggested standard features based on local needs and desires. The experiences of counties currently automated, or in the process of automating, should be studied in this step.

2. Select the best option for system implementation

At this point, there appear to be three options for implementation of an automated magistrate system. One of these options should be selected based on several factors, including: cost effectiveness, ability to meet standard needs, ability to meet individual county needs, availability for timely implementation, and compatibility with AOC needs.

AOC In-house Development

The AOC could develop and implement an automated magistrate system for those counties who currently do not have one. This would require the AOC to dedicate extensive staff time to both development and implementation, and training (see cost section below).

Adaption of an Existing Local System

The AOC could assist counties in using a leveraged design approach. Counties could select and adapt an existing automated county system such as, Buncombe or Mecklenburg County. Most of the work has already been done by the originator of the system selected. However, the work is of a proprietary nature and may not meet the hardware available or the specific local needs of an area.

If an existing system is deemed appropriate, individuals from the selected county could be asked to serve as technical advisors to those interested in "importing" their system. There is still some developmental cost associated with adapting the system. Another significant cost is the purchase of needed hardware.

Purchase Vendor Software

The AOC could assist counties in selecting and purchasing an existing vendor system, such as, Vision Software and JALAN. This option requires the purchase of needed hardware and the vendor software. This option could be state funded and directed, locally funded and controlled, or some shared cost structure.

3. Develop and implement magistrate training

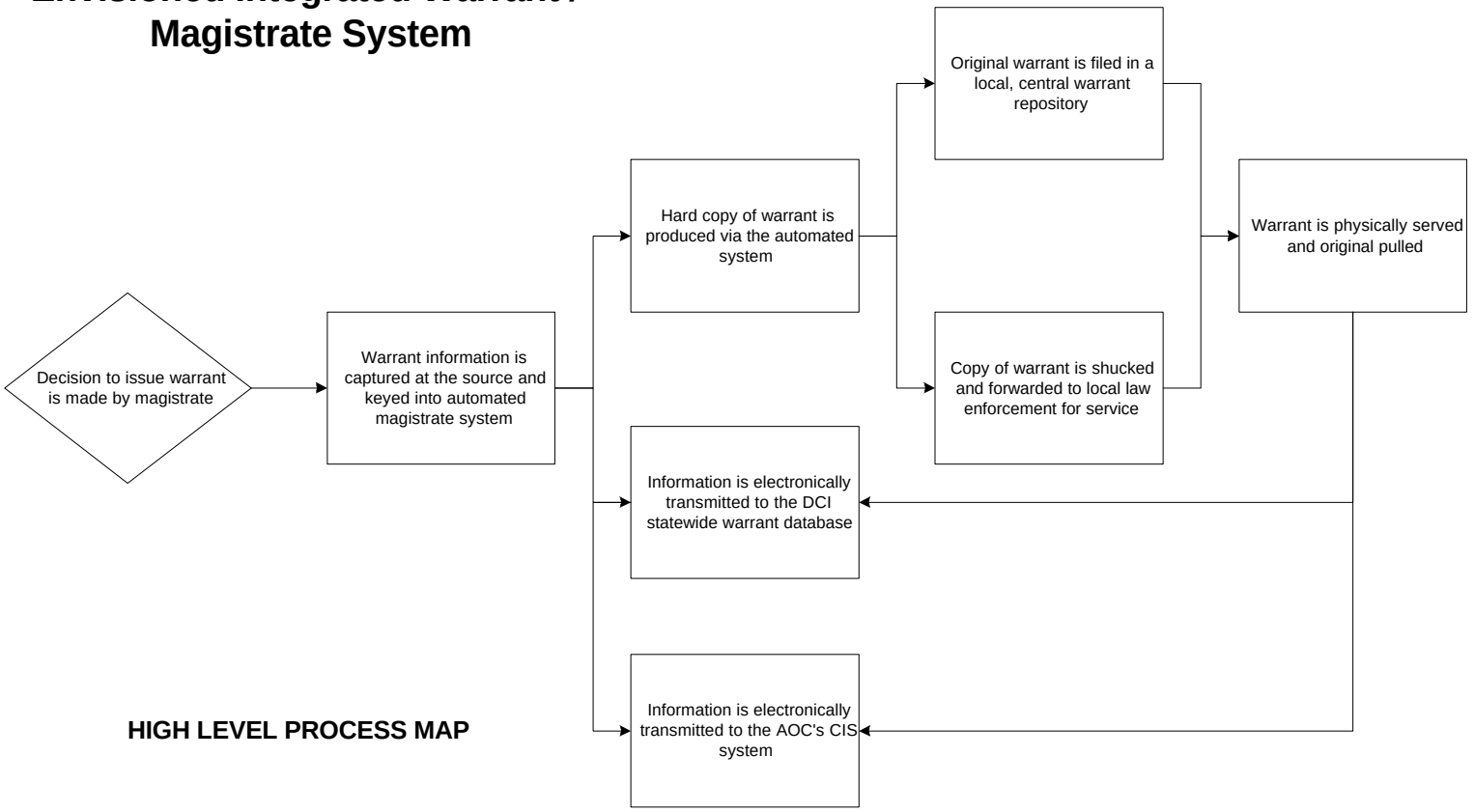
All magistrates will need to receive training on the use of any new automated system. This initial training may be provided by AOC, other magistrates who are currently automated, or a selected vendor. Once the initial training is conducted then a standard training package should be incorporated into the new magistrates' training. Computer-based training is also a possible solution once standardized training has been developed and implemented.

Implement AOC and DCI interface with a two-way feed back and forth between each system

The AOC should complete linking current automated magistrate systems to the CIS system through the efforts of the AOC's Local Interface Project. Issues still needing resolution, such as CIS system capacity and batching requirements will need to be addressed throughout the course of this initiative. Once all issues are resolved and the project interfaces are successfully operational, the AOC should begin the interface process with other counties as they become automated. Implementation statewide will allow all the magistrate systems and the CIS to feed disposition and warrant information back and forth; the goal being real time transmissions and updating.

Ideally, each automated magistrate system would be linked with the DCI system to feed arrest warrant information back and forth on a real time basis. The proposed links to AOC and DCI allow the magistrate to enter information on-line. The entered information flows in an immediate and simultaneous manner to the court system and the law enforcement community.

Envisioned Integrated Warrant / Magistrate System



HIGH LEVEL PROCESS MAP

FigureVI.7-1

Benefits

An automated magistrate system allows magistrates to produce warrants and other processes on a real time basis and reduce the amount of effort required to produce a single process. Standardized language formerly written for each warrant could be automatically filled in upon the keying of certain codes in predefined fields. It would also reduce inefficiency by eliminating redundant data entry and free-up clerk time currently spent reentering warrant information into the AOC's CIS system. In addition, accuracy of information will be improved by virtue of data only being keyed a single time.

Standard offense codes keyed into the system by a magistrate, tied to the appropriate statutory citation and structured sentencing information, could be printed directly on the documents. Magistrates would no longer have to look up sentencing information from manual tables. This would reduce the propensity of errors in sentencing information included on the warrant. Also, statewide offense code changes could be put into place more quickly by updating an automated system[1].

[1] The statewide offense master database would need to contain automatic links to sanctioned NCIC offense codes so that warrants which need to be extradited can be forwarded to NCIC.

Initial Cost Estimates

Cost Components	Internal Development ($)	Leveraged Implementation ($)
Hardware[2]	500,000	500,000
Database	300,000	300,000
Software Licensing/Source Code[3]		2,000,000
Software Development [A]	2,728,000	
Software Implementation[4]	528,000	528,000
Business Process Analysis[5]	396,000	396,000
Project Management[6]	528,000	528,000
Total	**$4,980,000**	**$4,252,000**

[2] Incremental mainframe upgrade.

[3] Includes source code, customization, and training.

[4] Requires two full time equivalent for one year at $22,000 per month.

[5] Three full time equivalents for 6 months at $22,000 per month.

[6] 24 Months of project management at $22,000 per month.

Ongoing Cost Estimates

Cost Components	Internal Development (Annual $)	Leveraged Implementation (Annual $)
Maintenance	777,000[7]	395,000[8]
Training[9]	528,000	528,000
Total	**$1,305,000**	**$923,000**

[7] 25% of the custom software development cost, 15% of the database cost, and 10% of the hardware cost.

[8] 15% of license or purchase cost of database and software and 10% of the cost of the hardware.

[9] Assumed 10% turnover of magistrate staff requires two full time equivalents throughout the year.

A. Custom Software Development

Task	Months	People	Total
Analysis	4	3	12
Design	4	3	12
Development	12	5	60
Testing	4	5	20
Conversion	4	3	12
QA	8	1	8
		Total Person Months	**124**
		Total Cost	**$2,728,000**

STATEWIDE IDENTIFICATION INDEX (SII)

CURRENT SITUATION

North Carolina does not have an automated, integrated statewide identification index (SII) based on the State Identification Number (SID) that links together all records of a subject's involvement with the criminal justice system.

RECOMMENDED SOLUTION

Establishment of a Statewide Identification Index (SII) which supports the following:

- Built on positive subject identification and will be SID and fingerprint based.
- Rapid identification of a subject's involvement with the criminal justice system.
- Graphical, intuitive subject search, and identification process.

Three categories of information will be provided through an inquiry into the Statewide Identification Index:

- Visual warning flags for items requiring immediate user notification (e.g. in-jail, on-probation, warrant).
- Subject demographic information including physical descriptors and address history.
- An index of, and eventual automatic electronic linkage to, a subject's criminal activity and related source documents (e.g. arrests, court cases, prison stays).

Current Situation

North Carolina does not have an integrated, automated, statewide identification index based on the State Identification Number (SID) that links together all records of a subject's involvement with the criminal justice system. Many of the state and local systems have an automated name search capability that is specific to that particular function. For instance, there is a name search capability in the AOC Court Information System, there is one in the DOC Prison System, and there is one in each of the counties with jail information systems. It is incumbent upon the user, however, to first identify which system(s) will have the information needed and then to individually search these systems, one at a time.

A Statewide Identification Index is a method of maintaining a subject identification information index which includes names and other identifiers for all persons about whom a record is held somewhere within a state or local criminal justice system. The automated name index is the key to rapidly and accurately identifying a person's current and past involvement with the criminal justice system as well as providing automated or manual linkages to the identified source documents.

Recommended Solution

CJIN requires establishment of a SII which links together incidents, arrests, court cases, dispositions, inmates, treatments, victims, custody status, and release data. SII presents person based information - all criminal activity records for one person are combined into one SII record. This is in comparison to event-based information, where a separate entry is presented for every incident and no attempt is made to consolidate records together for the same person.

The following section describes the SII approach recommended, the information needs that will be met by SII, and the application phases for development of SII.

Approach

1. SII will be built on positive subject identification and will be SID and fingerprint based.

A SII can be built on positive identification based records (fingerprints), possible identification based (non-fingerprint demographic information), or both. For purposes of this document, SII will refer to a *positive* identification based system and Master Name Index (MNI) will refer to a *probable* (non-fingerprint based) identification based system. The advantages and disadvantages of each method are discussed below.

- *Positive Identification Based SII (Fingerprints)*

A positive identification SII includes only subject records which have been identified through fingerprinting or another equally accurate personal identification method. The advantages to using only positive identification based records is the certainty of subject identification to the user. The disadvantage of this approach is that SII information is not provided on many other subjects who come in contact with the criminal justice system, but do not have fingerprints taken. Under current practices in the state, this would eliminate the inclusion of most misdemeanant, witness, victim, and juvenile subjects in the SII.

- ***Probable Identification Based MNI (Non-fingerprint demographics)***

A probable identification MNI includes subject records which have been identified through a rigid matching of key demographics. Most jurisdictions using this method require that the name, sex, race, and date-of-birth match between two records in order for them to be linked together as the same person. If this information cannot be matched, then a new subject record is created. The advantage to this approach is that subjects who have not been fingerprinted, but are still involved with a criminal justice event, are included in the MNI. This can include all arrestee records, as well as witness, victim, suspect, and even juvenile records with sufficient demographic data. There are two disadvantages to

this method:

- Records belonging to two different people with the same apparent demographic data may be matched and result in incorrect arrest, charging, or sentencing decisions (i.e. one person is arrested for an outstanding warrant on another person).

- Records belonging to the same person with different demographic data may not be matched, resulting in the omission of key criminal activity information when making arrest, charging, or sentencing decisions. Aliases are not automatically linked with this method.

Our recommendation is that the initial implementation be a positive identification, fingerprint record based State Identification Index (SII).

After the stabilization of the SII based on positive identification has occurred, the process of creating a separate but linked Master Name Index (MNI) based on *probable identification* can begin. The probable identification MNI provides a powerful tool in the linking of non-fingerprinted subjects who have involvement with the criminal justice system.

2. SII will provide rapid identification of past and current involvement with the criminal justice system statewide.

A Statewide Identification Index provides a central inquiry and identification point for all users to access any information regarding a subject's activity with the criminal justice system.

3. SII will provide a graphical, intuitive subject search and identification process.

In order to be effective, SII must provide the user with uniform presentation of subject demographic information and warning flags. Additionally, SII must provide an easy, quick method for accessing source documents in other systems

that support the SII.

SII Information

Three broad categories of information will be included in the Statewide Identification Index :

1. Warning Flags

The Statewide Identification Index will provide warning flags that will immediately notify the user of specific conditions regarding this subject. These warning flags will be visually prominent and will be used to indicate subject status information which is of highest importance to the user. Initial recommendations for these warning flags include:

- ***In Prison or Work-Release Warning Flag***
  A visual warning indicator that the subject is currently in a state prison or on work-release from a state prison and the prison facility location.

- ***In Jail Warning Flag***
  A visual warning indicator that the subject is currently in a county jail and the jail facility location.

- ***Outstanding (Unserved) Warrant Flag***
  A visual warning indicator that the subject has one or more outstanding warrants.

- ***On Probation Flag***
  A visual warning indicator that the subject is currently on probation and the name of the probation officer's agency.

- ***Felony Conviction***
  A visual warning indicator that the subject has at least one felony conviction.

2. Demographics

The SII will provide up-to-date subject demographics. We recommend that this includes name (first, middle, last, suffix), sex, race, date-of-birth, state identification number (SID), FBI number, driver's license, social security number, and residential and employer addressees. It will also provide for alias versions of all this information.

3. Index of Criminal Activity Information

The SII maintains an index of a subject's criminal activity and related source electronic documents that exist within the criminal justice community. It is also envisioned that SII will provide an automatic, electronic link to this information, regardless of its location in local, state, or national databases. The following lists the proposed indexes which SII would maintain. Also listed is the anticipated source of this information. A number of these records are not currently automated, especially at the local level.

- Prison Records - DOC prison booking and release
- Jail Booking Records - Local jails admission and release
- Warrants (Unserved and Served) - CJIN statewide warrant repository
- Criminal History - CJIN statewide criminal history repository
- Arrest/Incident Records - Arrests as reported to the SBI
- Court Cases - AOC Court Information System, Criminal Module
- Probation and Parole Cases - Probation and Parole case records
- Prosecution Cases - Prosecution Case Records
- Imaging Records - Mugshot Systems

SII will contain all occurrences of the above events, including the key identification number (e.g. court case number, arrest number) as well as the associated agency with each incident.

SII Applications

The SII application is envisioned to be a newly developed or vendor purchased system. There are three major application development phases to this project:

1. SII inquiry functions and database

This phase addresses development of all screens and reports that provide the user interface for access to information contained within SII. This includes the query screens by name and other demographics, as well as alias matching software.

2. SII subject event update processes

This phase involves creation of the processes which will update the SII system with needed information at key points of the subject's path through the criminal justice system. This phase is probably the most difficult of the three and will spawn a series of projects to begin collection of this information in some cases, and then updating this information to SII.

3. SII automated links to external criminal activity records

This phase addresses the creation of automated links from SII to source documents in an external system. For instance, a user inquires on a subject, requests to view a list of current court cases, and then upon selecting a particular court case

is provided the full source document detailed on the selected court case as it exists in the AOC system.

Project Dependencies

- CJIN Security Project
- TCP/IP Project
- End-User Technology Upgrade Project
- Statewide Automated Fingerprint Identification System Project

Initial Cost Estimates

Cost Component	Internal Development ($)	Leveraged Implementation ($)
Hardware	1,000,000[1]	1,000,000
Database	500,000	500,000
Software Licensing/Source Code		500,000
Software Development[A]	3,696,000	2,156,000
Software Distribution[2]	500,000	500,000
Business Process Analysis[3]	264,000	264,000
Project Management[4]	792,000	792,000
Total	**$6,752,000**	**$5,712,000**

[1] Estimated cost of minicomputer to support functionality.

[2] Distribution includes courts, corrections, and law enforcement agencies.

[3] 2 Full time equivalents(FTE) for 6 mos.

[4] 1 FTE for 3 yrs.

Ongoing Cost Estimates

Cost Components	Internal Development ($ Annually)	Leveraged Implementation ($ Annually)
Maintenance[5]	1,099,000	250,000
Training[6]	264,000	264,000
Total	**$1,363,000**	**$514,000**

[5] Maintenance is estimated at 10% of the initial hardware cost, 15% of the database cost, and 25% of the internal software development cost for internal development. The estimate for leveraged implementation is 10% of the hardware and 15% of the database and software costs.

[6] Ongoing training will require one FTE.

A. Custom Software Development

A1. Inquiry Database

Task	Months	People	Total
Analysis	3	2	6
Design	3	2	6
Development	6	2	12
Testing	3	3	9
Conversion	3	3	9
Total Person Months			**42**
		Total Cost	**$924,000**

A2. Subject Event Update Process

Task	Months	People	Total
Analysis	4	2	8
Design	4	2	8
Development	8	2	16
Testing	4	3	12
Conversion	4	3	12
Total Person Months			**56**
		Total Cost	**$1,232,000**

A3. Automated Links to Subject Update Process

Task	Months	People	Total
Analysis	3	2	6
Design	3	2	6
Development	6	2	12
Testing	3	3	9
Conversion	3	3	9
Total Person Months			**42**
		Total Cost	**$924,000**

A. Total Software Development

Task	Months	People	Total
Inquiry Database			42
Subject Event Update Process			56
Automated Links to Subject Activity Records			42
Training	6	2	12
QA	16	1	16
		Total Person Months	**168**
		Total Cost	**$3,696,000**

STATEWIDE INTEGRATED CRIMINAL HISTORY REPOSITORY

CURRENT SITUATION

Criminal justice information users must search separate systems in order to obtain comprehensive statewide criminal histories.

- The SBI / DCI system relies on an individual's fingerprints to assign a unique statewide identification number (SID). The SBI / DCI system contains fingerprinted felony and serious misdemeanor arrest, court and custody information.
- The AOC maintains all court disposition information.
- DOC maintains conviction information on fingerprinted and non-fingerprinted offenders in prison, or on probation and parole.
- Some local agencies maintain their own criminal history databases which may or may not contain fingerprint information.

NEED FOR CHANGE

- Misdemeanor crimes comprise the majority of arrests and convictions in the state, however, only fingerprinted serious misdemeanor offenses are included in the SBI / DCI criminal history system.
- Law enforcement officers cannot quickly and easily access criminal history information in the field. Officers need to quickly know if someone is wanted and / or dangerous when making decisions on approaching or apprehending suspects and offenders.
- Magistrates and district attorneys do not always have an offender's complete criminal history which is essential in making charging, bail, and release decisions.
- Judges rely on criminal history information for making sentencing determinations. Inaccurate or incomplete information may result in criminals not receiving suitable sentences.
- Without adequate criminal histories, the Parole Commission is unable to affix appropriate conditions of probation and parole, which could result in criminals being returned to the community without the correct level of supervision or restrictions.
- Non-criminal justice users such as employers, firearm dealers, and other government agencies require timely and comprehensive criminal history information for employment screening, firearm purchases, and security clearance screening.
- Without a positive identification process, it can from take several hours to several days to extract, sort, and analyze criminal history information generated by the various criminal justice systems.

RECOMMENDED SOLUTIONS

- Fingerprint all misdemeanants
- Expand DCI's current criminal history repository to include all misdemeanor offense and disposition information.
- Develop standardized, user-friendly formats for viewing information.

Current Situation

Although North Carolina has one of the most up-to-date computerized criminal history record systems in the country, no single, comprehensive statewide criminal history repository exists in the state. Criminal justice information users must now independently search multiple, separate criminal history databases. Even though an abundance of criminal history information exists in these different systems, in order to compile a comprehensive picture of an offender's criminal history, key pieces of information often have to be gleaned from one or more databases.

- The State Bureau of Investigation's (SBI) Division of Criminal Information (DCI) maintains a felony and serious misdemeanor fingerprint-based criminal history repository. It generally does not contain arrest and disposition information on misdemeanors. This results in the majority of misdemeanor convictions not being available to users querying this system.
- The Administrative Office of the Courts (AOC), through their Court Information System (CIS), maintains disposition information for all court cases. Because AOC receives the SID number when reporting court disposition to DCI, CIS users can link cases by either SID or check digit number. Since CIS does not have SIDs for most misdemeanor offenses,

CIS users must search using name only, or name plus date-of-birth, which often results in multiple responses that the user must cull through and analyze.

- The Department of Correction (DOC) maintains a computerized data system that contains criminal history information as it relates to fingerprint based imprisonment, probation, and parole status.

- A number of counties have local information systems that capture criminal history information on offenders. These systems are limited in that they may not contain fingerprint or statewide identification number (SID) information. They are further limited in that they may only contain information on offenses committed within their geographic boundaries; information that is not currently accessible on a statewide basis.

Even when information from these different systems is retrieved it is often inconsistent, incomplete, and may contain errors. Because of differing information needs across agencies, diversity in format, and terminology, the variety of the content of the records is considerable. This creates problems for both in-state and out-of-state users when attempting to decipher codes, abbreviations and formats.

Current Criminal History Query Process

Determining actual and elapsed time estimates for retrieval of automated criminal case history information is an extremely variant process. The amount of time it takes for a judge, magistrate, district attorney, police officer, or other criminal justice professional to obtain criminal history is dependent on a host of variables including:

- electronic access to various agency databases
- the skill level of the person querying the system
- the amount of identifying information provided (delimiters)
- the priority of the inquiry and the existing backlog of requests

Under ideal circumstances, a skilled user with immediate access to the AOC, DCI, and DOC databases, who has positive identification on an individual in the form of an SID number, could generate comprehensive criminal history information

in a matter of minutes[1]. However, if the user has to share access to the terminal / databases with numerous other users, or has no access to a terminal and must call another agency or location that does, this increases the elapsed time involved in attempting to retrieve information.

Further, if the user does not have a positive identifier and only a name is known, and the name is a common one, then the information generated by a search of the various criminal justice information systems including AOC, DCI, and DOC, may be voluminous and quite possibly meaningless. If more identifying information is provided, such as a name plus a date of birth, last known address, and / or race, sex, etc., the search results will be narrower, computer response time will be better, and less time will have to be spent attributing the appropriate record(s) to the appropriate individual.

Recommended Solutions

Expand DCI's centralized criminal history repository to include all adult misdemeanor offenses and disposition information.

In-state survey results indicated that 97% of respondents rated misdemeanor criminal history as extremely important or important.

Providing users with *complete and accurate* information must allow for the inclusion of misdemeanor offenses. For most counties, this information is currently available in the AOC's Court Information System. However, only those misdemeanor cases that have been fingerprinted (generally serious misdemeanors) are linked to a positive identifier such as a statewide identification number (SID). Without this positive identification it is often impossible to determine the accuracy of non-felony conviction information. Further, the wide-spread use of aliases by arrestees makes positive

[1] Even with positive identification in the form on an SID number, comprehensive criminal history information inclusive of misdemeanor offenses may or may not be available.

identification a necessary part of the criminal history process. It has been estimated that inclusion of misdemeanor arrests would increase the number of DCI criminal history records by 500%.

Develop standardized user friendly formats in which to view and analyze data/information.

The standardization of information collected by various criminal justice agencies is a key step in developing a comprehensive statewide criminal history database (see the Data Sharing Standards Project section VI.1 of this report). Focus group respondents echoed complaints of having to sort through voluminous data to extract meaningful information. Agencies also use different internal codes and abbreviations that may be unfamiliar to the user. The user should be able to view information in such a way that the product becomes a decision making tool. For example, an officer approaching a suspect in the field wants to immediately know if the person is a dangerous felon, has a history of resisting arrest, or has outstanding warrants. During an investigation however, that same officer may want a suspect's entire criminal history. The state of Maryland provides an optional narrative criminal history format that has received positive feedback from users.

Strengthen statutory language to mandate fingerprinting individuals charged with misdemeanor offenses

According to the Bureau of Justice Statistics' Use and Management of Criminal History Record Information, from a judicial viewpoint, the lack of comprehensive misdemeanor criminal history information has been identified as a major deficiency of current systems. N.C.G.S. §15A-502 allows for fingerprints and photographs to be taken in misdemeanor cases when an individual has been arrested or committed to a detention facility, however, only a few counties currently do this. Focus group participants agreed that this is because of a lack of resources rather than an unwillingness on the part of law enforcement to fingerprint all arrestees.

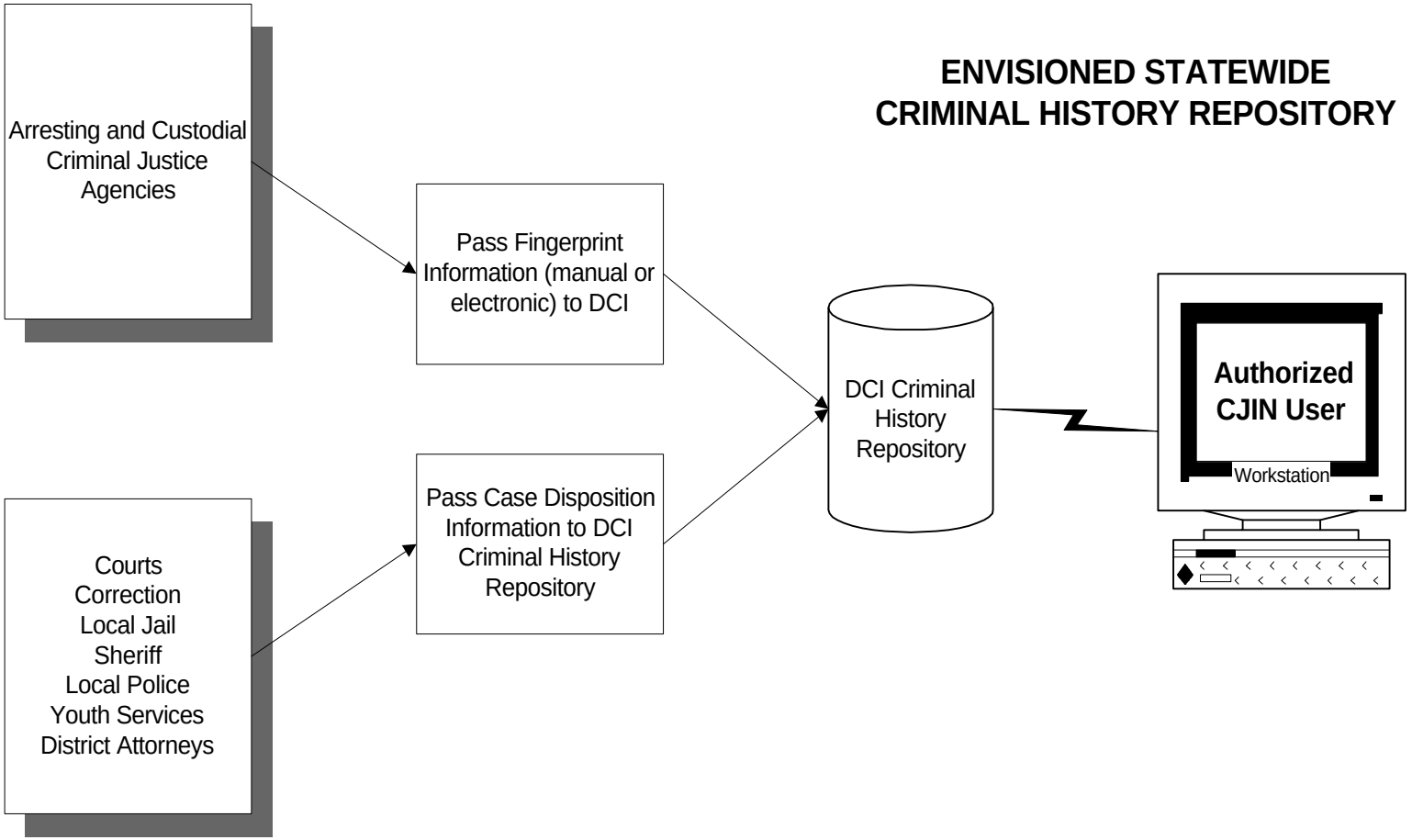

ENVISIONED STATEWIDE
CRIMINAL HISTORY REPOSITORY
Arresting and Custodial Criminal Justice Agencies
Courts
Correction
Local Jail
Sheriff
Local Police
Youth Services
District Attorneys
Pass Fingerprint Information (manual or electronic) to DCI
Pass Case Disposition Information to DCI Criminal History Repository
DCI Criminal History Repository
Authorized CJIN User
Workstation

Figure VI.9-1

The options presented below were evaluated as potential alternative recommendations, but due to various factors described herein, they were not thought to be implementable in the near-term.

Additional Long-term Options

Option#1

Move toward a distributed criminal history approach.

North Carolina is currently only one of three states in the country participating in the FBI's Interstate Identification Index (III) National Fingerprint File (NFF) project. The goal of the NFF project is to eliminate the duplication of state criminal history and fingerprint information in the FBI's national repository. Where III and NFF are in place, the FBI system merely acts as a "pointer", electronically directing the out-of-state requests to the appropriate state repository which is then responsible for re-routing that information back to the requesting state. This eliminates the need for entire duplicate records to be kept by both the federal and state government.

To expand that concept, a future migration away from centralized databases to distributed systems could be a goal for the state as well. In keeping with the goals of III and NFF, DCI's criminal history system could also act as a pointer, directing requests to other state agencies or local-level criminal history databases, eliminating the need for duplication at the state level. Implementation of this strategy is dependent on raising the accuracy and completeness of current local automated criminal history systems.

Option #2

Transfer responsibility of maintaining a statewide criminal history repository from DCI to AOC .

Since all of the disposition information that comprises a criminal case history arises from court related actions, a reasonable long-term (10 plus years) alternative strategy could be to migrate the responsibility of maintaining a statewide criminal history repository from DCI to the AOC. In doing so, the AOC would need to develop the capacity for including a positive identifier (SID) into its criminal case history system for all convictions and DOC incarceration, probation and parole information. The AOC would have to be brought up to FBI criminal history records standards and comply with additional national standards and procedures pertaining to the use and dissemination of records, response times, data quality, and system security. In addition, the AOC would need to provide a link to the national criminal history repository. Currently, the FBI wants only one Control Terminal Agency (CTA) per state. The AOC statewide criminal history repository would also need a link for updating data in the Statewide Identification Index (SII).

If the CJIN Study Committee wishes to adopt this long-term strategy, careful consideration needs to be given to the functionality, resources and goals of both the AOC and DCI.

Dependencies

- ***Data Sharing Standards and Common Definitions***

In order for a single comprehensive criminal database to be developed, data sharing standards, common definitions, and formats need to be established. These common standards are essential for both the collection and reporting of data if the information is to be of real value to the users. Time spent searching and analyzing data from disparate systems is inefficient and allows for misinterpretation and misidentification of criminal history elements that may be critical in the decision making process.

- ***Statewide Fingerprinting of Misdemeanants***

Consistency in fingerprinting misdemeanor offenses on a statewide basis would greatly enhance the comprehensiveness of criminal history records. Since misdemeanor offenses greatly exceed felony offenses, an accurate portrayal of an individuals' criminal history is not possible without inclusion of this information. In order to positively identify misdemeanants and include conviction information into a statewide criminal history database, consistent fingerprinting of misdemenants must be established.

Risks

- Concurrently bringing the AOC up to national criminal history certification standards while expanding the DCI criminal history databases for misdemeanants results in an interim duplication of effort and investment. However, this is necessary if the state elects to migrate toward the elimination of duplicate record storage at both DCI and AOC. There will need to be clearly developed plans for the migration of these information systems in order for maintenance of dual repositories to be as time-limited as possible. Plans to bring the AOC up to federal standards should be jointly developed with realistic and measurable goals and time frames.

  It is important to note that enhancing the SBI AFIS is not a duplication of effort and investment. Even if the AOC maintains the criminal history information files instead of DCI, there will still need to be a statewide AFIS system to assign the SID number based on fingerprint data.

- The AOC database does not have all the historical fingerprint supported data that is currently a part of DCI criminal history files. The state has a NFF agreement with the FBI to provide this data.

Benefits

Ideally, information that currently requires hours if not days of retrieval and analysis effort by magistrates, judges, law enforcement officers, district attorneys, and correction personnel could be generated in minutes or less. Access to timely, accurate, and understandable criminal history information will enable justice professionals to make more informed decisions at each stage of the justice process; reduce time spent collecting information from various sources; reduce the time spent entering identical data into separate systems; and enhance officer and public safety.

It is obvious that the current processes employed in the retrieval of criminal history information would be substantially reduced by introduction of an integrated, automated system. With appropriate staff training and wide-spread access to the new system by authorized users, the concurrent savings in labor-hours proves to be substantial.

Initial Cost Estimates

Cost Components	Development Cost ($)
Hardware[2]	500,000
Database	1,000,000
Software Development [A]	1,980,000
Software Distribution	360,000
Business Process Analysis[3]	396,000
Project Management[4]	528,000
Total	**$4,764,000**

[2] Incremental mainframe upgrade.

[3] Three full time equivalents (FTE) for six months. An FTE is costed at $22,000 per month.

[4] One FTE for two years.

Ongoing Cost Factors

Cost Component	Cost ($ Annually)
Maintenance[5]	695,000
Training[6]	264,000
Total	**$959,000**

[5] Maintenance is estimated at 10% of the initial hardware costs, 15% of the database costs, and 25% of the internal software development costs.

[6] Training costs assume one full time trainer for one year. Package implementation follows the same training cost structure since most package implementations on include a "train the trainer"component.

A. Custom Software Development

Task	Months	People	Total
Analysis	3	3	9
Design	3	3	9
Development	8	4	32
Testing	4	4	16
Conversion	6	3	18
QA	6	1	6
Total Person Months			**90**
		Total Cost	**$1,980,000**

STATEWIDE WARRANT SYSTEM

CURRENT SITUATION

The SBI's Division of Criminal Information maintains a statewide warrant repository that is not regularly used by some agencies for the following reasons:

Information is not updated in a timely manner

- Warrants that may have been recalled remain on the system because of a backlog of updates not yet entered into the system.
- Recently issued warrants may not have been entered yet, therefore, the information is unavailable to someone who queries the system.

The repository primarily contains felony warrants

- Misdemeanor warrants comprise the majority of processes law enforcement is responsible for serving.

NEED FOR CHANGE

- Both public and officer safety are severely jeopardized by an officer's inability to quickly and easily determine if a suspect has an outstanding warrant.
- Even when an officer knows that a warrant is outstanding, the warrant may be inaccessible, especially in counties that are not automated, and / or do not have a central repository that operates on a 24 hour-a-day basis.
- The vast majority of counties do not have automated systems and rely on local law enforcement agencies to manually enter the warrant information into both their local system and into DCI's repository from the hard copy document they receive from the magistrate.
- It may take days or weeks for a warrant to reach the appropriate law enforcement agency responsible for service due to various factors including; the level of automation and the amount time it takes to actually produce the warrant; staff levels and volume of warrants being issued.

RECOMMENDED SOLUTIONS

- Develop local centralized "hard copy"warrant repositories for 24 hour-a-day warrant retrieval.
- Link the proposed automated AOC magistrate system to the development of a centralized statewide warrant database to include misdemeanor warrants.
- Move towards a paper-on-demand arrest / warrant system in the future.

Current Situation

A central issue that was echoed by law enforcement, court, and correction personnel was the need for reliable, easily accessible warrant information. Officers, magistrates, district attorneys, and judges need this information in order to determine:

- whether or not to arrest an individual
- the appropriate number of charges when arresting
- pre-trial release conditions and bond amounts
- prosecution and defense strategies

In-State Survey Results

Our in-state survey results indicated that 95% of all respondents rated the need for information on outstanding warrants, on a statewide basis, as "very important" or "important", while 94% of law enforcement respondents rated this as "very important".

Criminal justice professionals are often unable to determine if a suspect or offender has outstanding warrants without calling individual police departments in some counties. Even though DCI maintains a statewide automated warrant repository, it is not regularly used. This is due to the information contained in the system not being the most up-to-date information available and its being primarily limited to felony warrants. Because officers feel they cannot always rely on the information contained on the statewide warrant database, the reliance on the actual physical warrant is firmly entrenched in current law enforcement processes.

Copies of the warrants produced by either the magistrate, judge, or grand jury are fowarded to the local law enforcement agency responsible for service and to the clerk. The reason information contained on the statewide warrant system is not regularly up-dated is due to delays in entering the information into multiple systems. At times, local law enforcement agencies do not enter information on some warrants into the DCI system at all.

- Local law enforcement is required to enter warrant information multiple times, including into their own local system if they have one, the DCI central warrant repository, and the FBI's NCIC system if it is a felony warrant. However, during the course of our focus groups it was explained that some local agencies don't enter information into the DCI system, and only into NCIC when required.

- The Clerk also enters warrant information into the AOC's CIS system which does not have linkages to either the DCI warrant repository, local law enforcement or NCIC systems.

This process represents tremendous redundancy raising the potential for errors and wasting valuable human resources.

Because magistrates are responsible for issuing warrants, the first step in the warrant process, we examined the possibility that the courts should be responsible for managing and maintaining the statewide warrant repository. However, since the need for accurate and timely warrant information is primarily a need of law enforcement, we recommend that the statewide warrant repository be managed and maintained by the SBI, with the necessary linkages to the AOC's CIS system.

Another reason the SBI / DCI system is seen as limited by law enforcement officials is that it is does not contain the majority of outstanding misdemeanor warrants. At the local level an additional problem is access to the actual warrant. In counties where there is no centralized warrant repository it may be difficult for officers to locate the actual warrant when a suspect or offender is identified. For example, an officer may have first-hand knowledge that a warrant has been issued for a individual, however the warrant itself may be in the possession of another officer or in transport between the magistrate court to the local agency, etc.

Recommended Solutions

Short-term Strategy:

- **Develop centralized local warrant repositories for 24-hour warrant retrieval**

In order to maintain appropriate control over the location of original warrants and other process documents the creation of a central warrant repository is a practical short-term solution. The initial start-up costs for development of this type of system are minimal. In those counties with 24 hour, 7 day-a-week central intake facilities, or dispatch centers, the

only costs would be for the storage space and filing system necessary to contain the processes. Buncombe County's system could be considered a model for other mid-size-to-large counties to adopt. Smaller counties may wish to regionalize their warrant repository and share responsibility for maintaining these documents.

Medium-term Strategy:

- **Link the proposed automated magistrate system to the warrant system**

Our medium-term strategy for enhancing current warrant processes is dependent on the implementation of the automated magistrate system. Once the proposed magistrate system is implemented, warrant information can be transmitted real-time directly into the SBI / DCI warrant repository, eliminating the need for law enforcement to be responsible for the data entry. Information will be captured at the source and the propensity for errors will be greatly reduced. Confidence in the information contained in the database is increased, thereby, making it a useful tool for law enforcement.

Long-term Strategy:

- **Migrate toward an automated "paper on demand" arrest / warrant system.**

Our long-term recommendation for optimized warrant process is to move to a paper-on-demand arrest/warrant system. An automated arrest / warrant system would allow law enforcement officers to arrest a suspect based on the knowledge that a warrant exists. A linkage between the automated magistrate system and local law enforcement agencies can provide law enforcement agencies with electronic notification when a warrant is issued. The agency responsible for service can print out a "log" of warrants to be served for a particular geographic area. The log would also contains physical descriptions and other identifiers that are necessary for the officer serving the warrant. The individual is served and brought before the magistrate and the officer completes the "return of service" which triggers the printing of the warrant which is then served to the offender. This way, the event or "service" is never separated from the act of updating the database by virtue of
having to print the warrant. By tying together the automated magistrate system with a paper-on-demand arrest / warrant system, the database is accurate, comprehensive and up-to-date. Therefore, confidence in the accuracy of the system is uncompromised and officers can rely on the fact that a warrant is current and can arrest an individual based on that knowledge.

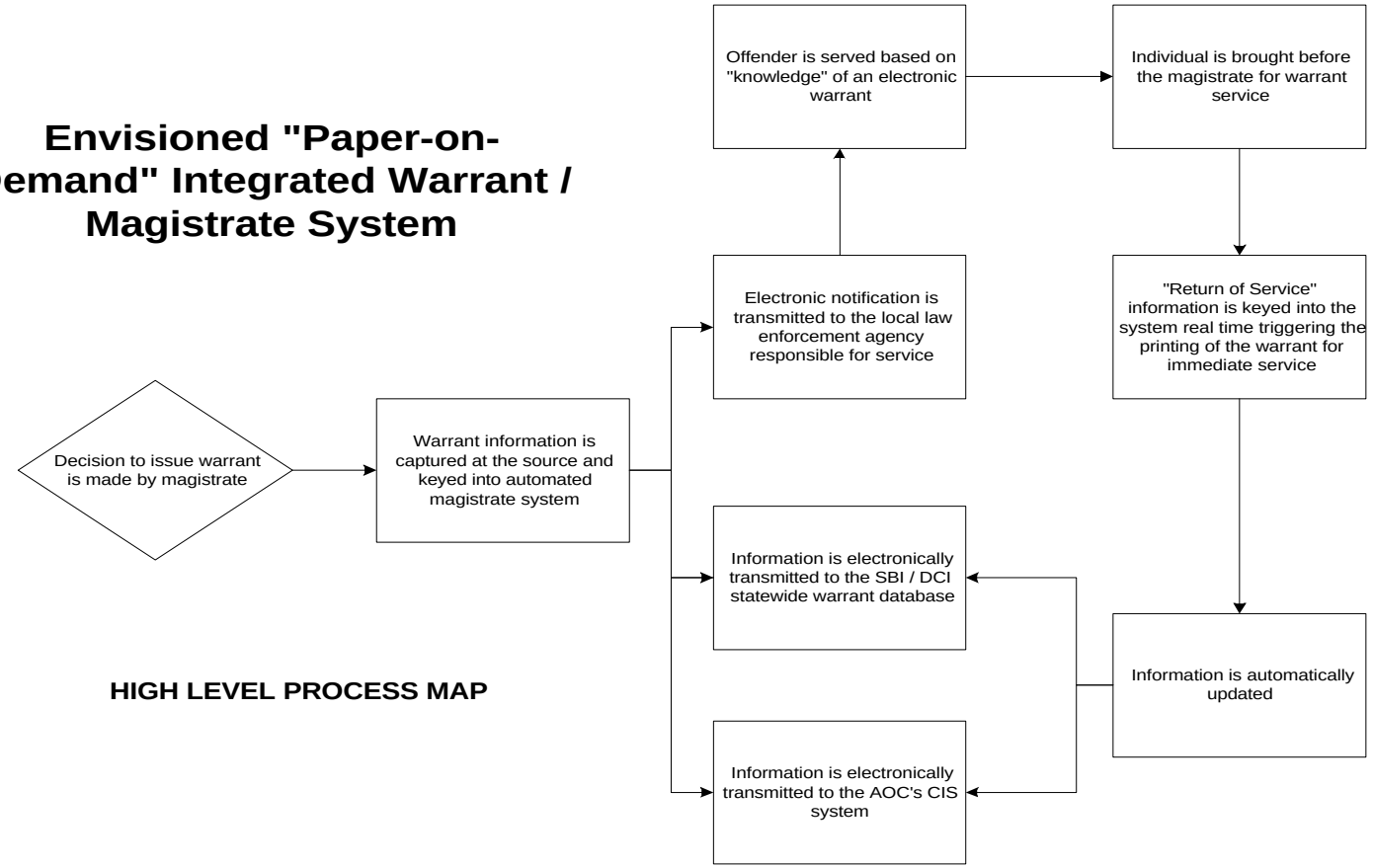


Figure VI.10-1

Initial Cost Estimates

Cost Components	Internal Development ($)	Leveraged Implementation ($)
Hardware[1]	500,000	500,000
Database	1,000,000	1,000,000
Software Development [A]	1,386,000	
Software License / Source Code / Conversion[2]		1,000,000
Software Distribution	360,000	360,000
Business Process Analysis[3]	396,000	396,000
Project Management[4]	528,000	528,000
Total	**$4,170,000**	**$3,784,000**

[1] Provides additional disk storage and offsets CPU upgrade cost.

[2] Includes license fee, source code and modifications.

[3] Three full time equivalents (FTE) for six months. An FTE is costed at $22,000 per month.

[4] One FTE for two years.

Ongoing Cost Estimates

Cost Components	Internal Development ($ Annually)	Leveraged Implementation ($ Annually)
Maintenance[5]	546,500	450,000
Training[6]	528,000	528,000
Total	**$1,074,500**	**$978,000**

[5] 25% of custom software development costs, 15% of the database costs, and 10% of the hardware costs.

[6] Training costs assume two full time trainers for one year. Package implementation follows the same training cost structure since most package implementations on include a "train the trainer"component.

A. Custom Software Development

Task	Months	People	Total
Analysis	2	3	6
Design	2	3	6
Development	6	3	18
Testing	2	3	6
Conversion	6	3	18
QA	9	1	9
Total Person Months			**63**
		Total Cost	**$1,386,000**

COURTROOM AUTOMATION

NEED FOR CHANGE

Courts in the state of North Carolina currently experience a number of information problems:

- Manual courtroom data capture results in timelags in AOC's CIS system entry.
- Redundant data entry is costly and results in mistakes.
- Information systems are not used strategically.
- Other criminal justice agencies experience difficulty in accessing court information.

RECOMMENDED SOLUTION

Establishment of a statewide courtroom automation project which supports:

- Real-time data input in the courtroom.
- Triggered forms generation.
- Automatic queues to next in process.
- Automatic updates to case history and register of actions.
- User-friendly, common views.
- A plan for changes to business process, and provides adequate training.

Need for Change

Courtrooms in the state of North Carolina are manual operations. Judges conduct hearings and trials while courtroom clerks take manual minutes of the proceedings. When the pace slows, during breaks, or at the end of the day, courtroom clerks manually generate notifications, forms, and orders. The handwritten minutes are forwarded to the Clerk's Office where staff inputs the same information into the Administrative Office of the Court's (AOC) Court Information System (CIS). Although there are clerk's offices that complete this input process in one day, it is not uncommon for it to take a week or more. In some counties there are currently backlogs of three to four weeks.

In-state survey results indicated that 93% of court respondents rated the capture of disposition information in the courtroom as extremely important or important.

Manual courtroom data capture results in timelags in AOC CIS system entry

Information regarding court proceedings is not made available in a timely fashion causing delays in the provision of post-court services. Delays are caused by the need to transport documents to the next step in the process; queues in inputting information into automated systems, which are in large part due to staffing shortages or management issues in clerks' offices; and batch update programs.

Delays in data input of court proceedings and the production of the corresponding forms can result in the following situations:

- **Judges** do not know about a defendant's court activity throughout the state. Judges need to know if the defendant has pending court dates, and outstanding warrants for failures to appear. Structured sentencing guidelines require judges to know a defendant's prior criminal record. If clerks' offices are not updating this information in a timely manner, then judges may be making decisions based on incorrect information.

- **District Attorneys** do not know about a defendant's court activity through the state. District Attorneys need to know a defendant's prior criminal record when making decisions regarding charges and plea bargains.

- **Law enforcement agencies** do not know an offender's most recent criminal case history.

- **Jails** are not always aware that an offender has a future court date because some court dates pass before they have been input into the AOC's CIS system.

- **Jails** may not know that an inmate is being committed to state prison, and do not receive copies of judgments and commitment orders in a timely manner. As a result, it is not uncommon for an inmate to sit in jail for over a week when the inmate could have been sent to a state prison. This is a significant issue because many North Carolina jails are overcrowded, and less serious offenders may be released back into to the community in order to comply with occupancy limits.

- **Probation and Parole Officers** do not know if an offender has had probation or parole revoked.

Redundant data entry is costly and results in mistakes

Subsequent hand-offs and delays in entering courtroom transactions result in recordkeeping problems due to redundant processes, errors, and duplication of effort. Inadequate quality controls and methods for source data capture impairs the courts' ability to provide accurate, timely and complete case information.

Information systems are not used strategically

Most information is not accessible or shared between the courts' and other criminal justice agencies' computer systems. The agencies that have automated systems are re-entering the same information that the clerk has already entered into the AOC's CIS system. This duplication of effort when entering and maintaining case information often results in incomplete and inconsistent records.

Examples of duplicate data input include:

- Commitment Orders for defendants sent to state prison. There is no electronic interface to the Department of Correction (DOC) although there are future plans to send batch extracts of disposition information from AOC to DOC.

- Probation violation revocations are currently entered by AOC and DOC.

Other criminal justice agencies experience difficulty accessing court information

Automated systems do not talk to each other; various agencies have trouble sharing and transferring information. The difficulty in information sharing stems from the use of multiple identification and case numbers throughout the criminal justice system.

- Local law enforcement agencies need other jurisdictions' jail information, such as offender location, custody status, and release. Currently this information is collected through phone calls. Local jails want dynamic data exchanges with the AOC.

- Currently, police departments have no way to electronically track the disposition of misdemeanor cases. They must physically go to the clerk's office, reference a specific case, the clerk then prints the case from the AOC's CIS system, and police staff input the relevant information into their own system. Police agencies are interested in producing management reports from data that is currently being captured on the number and type of dispositions by officer.

Recommended Solutions

Real-time data input in the courtroom

Provide a system that allows transactions from court proceeding to be recorded in the courtroom exactly when they happen, not later when they have to be transcribed from a courtroom clerk's handwritten notes.

Triggered forms generation

Input should automatically trigger the generation of notices and forms, so that they can be printed and distributed in the courtroom. Judges should have the capability to electronically review forms and orders, and then affix an electronic signature with the use of a personal identification number.

Automatic queues to next in process

Queue workflow and electronic documents through the case process. Disposition information should be transmitted real time to divisions within the clerk's office, such as accounting, and to other criminal justice agencies, such as jails and prisons so they can respond to changes in an offender's custody status.

Automatic updates to case history and register of actions

Input should also automatically update the criminal case history database and the case register of actions.

User-friendly, common views

Judges and court staff should be able to logon in any courtroom in the state and have access to the same information presented in a user-friendly format. The clerk will have primary data input responsibilities and the judge can view this process or use the computer to perform inquiries during the proceeding.

Courtroom automation should include the following functional capabilities:

- Preparing for a session of court
- Recording the attendance of participants
- Identifying defendants who need to be fingerprinted
- Producing minutes
- Capturing juror names
- Tracking juror attendance
- Recording evidence details
- Producing document identification
- Processing and filing new documents
- Calculating fines and restitution payments
- Queuing payments to accounting
- Inquiring on case history
- Inquiring on criminal history
- Adding, deleting, or continuing cases on the docket
- Calling or activating a case for a hearing
- Capturing oral motions and results
- Recording rulings and orders
- Scheduling hearings
- Producing forms, orders, and notices
- Producing failure to appear warrants
- Tracking counsel challenges to jurors

- Preparing jury instructions
- Processing and filing new documents
- Posting events to the case register of actions[1]
- Recording and updating bail status
- Recording legal representation details
- Resetting cases

Plan for changes to business process, and provide adequate training

Provide judges and staff with the resources and training necessary to operate automated courtrooms. Plan for the changes that will result from the implementation of computers in the courtroom, including reengineering the courtroom business processes, redeploying staff to support the new processes, and training not only on using the system, but also on the skills needed for working in the new environment.

Benefits

Savings made from eliminating redundant data entry can be used to tackle other workload backlogs in the clerk's office. For example, we heard that there are huge backlogs in updating warrant records when fines are paid off. This greatly impacts law enforcement agencies, which assumes warrants are valid when there is a high probability that they are not.

By implementing real-time entry of courtroom transactions, the courts will provide enhanced service to other criminal justice agencies, and to the public at large.

[1]Posting is a term used to describe a process the computer performs behind the scenes.

- Judges will have access to case information when they need it. Information will be accurate, up-to-date, and without errors due to time lags in processing documents or completing data input. Moreover, all information will be provided to judges in an easy, user-friendly manner.

- By providing information in a more timely manner, users internal to the courts, as well as the other members of the criminal justice community, will have the ability to access accurate, up-to-date information about pending court cases in other jurisdictions, future court dates, warrants, and disposition of cases.

- By knowing the status of defendants, the courts can be more assertive about taking care of their outstanding business, such as warrants, scheduling, and outstanding fines, while they are in the courthouse.

- Agencies will be able to improve their ability to actively manage their resources. By getting real-time disposition information, the jails and prisons will be better able to forecast and plan their bedding needs.

- Courtroom generation of forms will increase the clerk's productivity.

- Generating judgment and commitment forms in the courtroom, having judges sign them that day, and electronically transmitting them, will eliminate the current hand-offs. This will reduce the processing time, and speed the process of moving offenders from local jails to state prison.

Recommended Applications / Technology

The AOC should implement a software application to automate all courtrooms. It should be graphical user interface (GUI) based, PC-based, and on a local area network. We recommend three procurement options:

- Expand the AOC Forms project that is currently being developed.

- Adapt software that has been developed by another state.

- Purchase a software package from an outside vendor and modify it to meet the needs of the AOC.

Business Process Changes

Redesign business process to take advantage of capturing information at the source through real-time data entry. It is critical that the courts do not merely automate current tasks that can be eliminated or processes that can streamlined. Manual tasks that will be accomplished with the computer, or "behind the scenes" by technology, must be eliminated. Savings in time and effort will not be realized if the courtroom clerk attempts real-time data entry while maintaining the traditional tasks and processes of doing business. There must be extensive participation by staff from high, medium, and low volume courts and courtrooms, during the redesign of business processes, application development, and implementation.

One of the keys to success of automating the courtroom will be achieving active participation of the judges during the redesign of courtroom processes, development of the software, and implementation. Judges must understand the way that information will be captured and how their behavior impacts this process. For example, in high volume courtrooms this may require a change in the way judges currently control the pace of the docket.

Initial Cost Estimates

Cost Components	Internal Development ($)	Leveraged Implementation ($)
Hardware	3,000,000[2]	3,000,000
Database	1,250,000	1,250,000
Software Licensing / Source	N/A	1,500,000
Software Development[A]	3,036,000	N/A
Software Distribution	1,000,000	1,000,000
Business Process Analysis[3]	792,000	792,000
Project Management[4]	1,056,000	1,056,000
Total	**$10,134,000**	**$8,598,000**

[2] Allocation for incremental mainframe performance upgrade.

[3] Three full time equivalents (FTE) for one year. An FTE is costed at $22,000 per month.

[4] Two FTEs for two years.

Ongoing Cost Estimates

Cost Components	Internal Development ($ Annually)	Leveraged Implementation ($ Annually)
Maintenance[5]	1,184,000	880,400
Training[6]	792,000	792,000
Total	**$1,976,000**	**$1,672,400**

[5] For custom development, maintenance is estimated at 10% of initial hardware cost, 10% of database cost, and 25% of software development cost. For leveraged implementation maintenance is estimated at 10% of initial hardware cost, 10% of initial database cost, plus 15% of software development cost.

[6] Training costs assume three full-time trainers for one year. Package implementation follows the same training cost structure since most package implementations include a "train the trainer" component.

A. Custom Software Development

Task	Months	People	Total
Analysis	4	4	16
Design	4	4	16
Development	6	4	24
Testing	4	6	24
Conversion	4	6	24
Training	6	3	18
Quality Assurance	8	2	16
		Total Person Months	**138**
		Total Cost	**$3,036,000**

AUTOMATED JUVENILE RECORDS

CURRENT SITUATION

Various juvenile criminal records span law enforcement, AOC's Juvenile Services, and the Department of Human Resource's (DHR) Division of Youth Services (DYS).

The SBI's Division of Criminal Information (SBI / DCI) collects crime statistics, excluding offender names, as part of the national Uniform Crime Reporting (UCR) program. Through the UCR program, statewide juvenile crime trends are measured by the number of arrests. Due to the nature of juvenile crime, some law enforcement agencies may be inconsistent in their level of reporting this information.

Juvenile court counselors maintain involvement with a juvenile through all aspects of the juvenile justice system. The juvenile court counselors are charged with collecting extensive information about juvenile offenders, such as, family history, educational records, medical services, etc. Information collection by juvenile court counselors is primarily a paper process. Some individual courts have automated selected records. Records are court-based and not available through any statewide database.

According to DYS, comprehensive juvenile background information may or may not be passed to them when a juvenile is adjudicated delinquent and committed to their facilities. Even if the collected information is passed to DYS it may not be as thoroughly documented as needed for evaluating the various needs of the juvenile. DYS maintains databases that are event-based, and track admission and release from detention facilities, training schools, and community-based alternative programs. DYS facilities do not have an automated on-line system to share information.

NEED FOR CHANGE

- There are duplicate data collection and recording efforts by juvenile court counselors, clerk of the courts, detention facilities, DYS central office, and individual training schools. The duplication wastes personnel time and increases the potential error rate with every entry into the system.
- Much of the data entry about juvenile offenders is completed manually which is very time consuming and difficult to retrieve by others who need the information.
- Through the UCR program, DCI analyzes juvenile crime data based upon the number of arrests reported by law enforcement agencies. While DCI collects juvenile arrests, it is not an offender-based reporting program. Due to the design and intent of the UCR program, the data collected provides limited benefits with regard to analyzing the effectiveness of juvenile treatment.
- DYS and AOC do not perceive the current level or effectiveness of information sharing the same. DYS feels that they do not always receive timely notification of commitments. Often they do not receive adequate background information about the juvenile upon commitment. DYS must locate and assign bed space on short notice which may or may not be the most appropriate "housing assignment" for the juvenile based on his / her needs and history. Counselors also must begin treatment strategies with very limited intake data.
- DYS facilities cannot share information on-line through any automated system. This results in time delays and lack of information sharing.

RECOMMENDED SOLUTIONS

- Conduct an audit of juvenile court counselor case files across the state. The audit will determine, 1) the level and consistency of detail in juvenile information collected, summarized, and forwarded to judges and other professionals charged with court ordered juvenile supervision, and, 2) the degree of standardization of reporting formats used across court jurisdictions.
- Automate all juvenile court case records using a statewide offender-based system.
- Automate all Division of Youth Services juvenile offender records.
- Establish an interface between the AOC, DCI, DOC, and DHR's DYS. The proposed juvenile AOC and DYS automation efforts must be compatible with the adult CJIN component. Proposed interfaces will eliminate duplication of data entry, generate reports based on aggregate data, and facilitate research on the effectiveness of juvenile treatment. Only authorized users will have access to information.
- Adopt a universal usage of a single, statewide, juvenile personal identification number to link a juvenile's record of arrests, court cases, dispositions, probation, custody, aftercare, and release data.
- Establish a Statewide Identification Index of juveniles which flags any item requiring immediate attention, such as, runaway status, subject demographic information, and other offense information.
- Fingerprint juveniles who are adjudicated delinquent and committed to DYS.

Current Situation

Various juvenile criminal records span law enforcement, AOC's Juvenile Services, and DHR's DYS. The General Assembly has funded a separate study that is also addressing information needs of the juvenile justice system. The first report from this study is due simultaneously with the CJIN Study.

Juvenile offender information is needed to:

- process individual offenders at all points of the system,
- determine the most effective supervision and treatment strategies for each offender,
- identify trends in juvenile crime, and
- assess the effectiveness of the current juvenile system.

Juvenile offender information is reviewed, collected, and forwarded to other agencies at various points in the process. Information collection is still primarily a manual process. Five core information issues exist: accessibility of data, duplicate data entry, lack of agency automation, lack of interagency automated interfaces, and lack of reliable statewide automated databases. This section describes the current information environment and the information issues that exist. Figure VI.12-1 provides a brief summary of the current information environment. The major steps of processing a juvenile from arrest through aftercare are addressed.

Figure VI. 12-1: Current Juvenile Information Environment

MAJOR PROCESS STEPS	AGENCY RESPONSIBILITY	INFORMATION ENVIRONMENT
1. Identify crime and apprehend juvenile offender	Local law enforcement agency	Generate initial police report: verified identity, offender information, and crime story.
1a. House juvenile in detention facility, if warranted.	DYS	Offender information and crime story.
2. Forward complaint to juvenile court	Local law enforcement agency	Forward initial police report and complete complaint to the court in the form of a Juvenile Petition.
3. Decide to accept and process juvenile petition	AOC, Juvenile Court Counselor	Complete intake card. Forward petition and intake card to the clerk. Initiate juvenile case record at the court level.
4. Process case and schedule hearing	AOC, Clerk of the Court	Prepare formalized petition. Issue summons for appearance.
5. Conduct hearing and adjudicate delinquent	AOC, Judge	Review all case information.

5a. Compile and summarize juvenile background information	AOC, Juvenile Court Counselor	Collect, summarize and submit report detailing juvenile offender background information, such as; education, medical history, family, etc.
6. Determine case disposition and issue court order	AOC, Judge	Review all case and juvenile background information
7. Record court order	AOC, Clerk of the Court AOC, Juvenile Court Counselor	Enter court order into AOC records. Enter court order into local court case file.
8. If placed on probation, supervise juvenile on probation	AOC, Juvenile Court Counselor	Collect relevant information to monitor juvenile readjustment to community.
8a. If committed, conduct DYS intake	DYS	Central office receives notification and information to complete one page data sheet. Intake is completed at training school. Receive and review court order and juvenile record information from the juvenile court counselor. Collect any needed background information not included in case file received.

9. Supervise juvenile in the selected residential setting	DYS AOC, Juvenile Court Counselor	Document relevant information about juvenile behavior and progress. Monthly contact with juvenile to monitor progress.
10. Release from DYS	DYS	Review court order and verify release date. Conduct release conference to provide relevant information to juvenile court counselor.
11. Conduct "aftercare" supervision of the juvenile in the community	AOC, Juvenile Court Counselor	Collect relevant information to monitor. Enter juvenile readjustment to community.

Law Enforcement

When asked about information needs, law enforcement officers and administrators consistently asked for more access to juvenile records. Currently, North Carolina statutes mandate very limited access to juvenile records. A law enforcement officer who encounters an adult can request criminal history information. The officer uses this information to assess any safety risks when face-to-face with an unknown entity. However, a law enforcement officer who encounters a juvenile is prohibited from accessing the juvenile equivalent of a criminal history. According to law enforcement officers, this impedes their ability to properly assess any immediate risk and places them in danger of potentially violent juvenile offenders.

A law enforcement officer who identifies a crime and apprehends a juvenile offender is responsible for the initial police report on the incident. Based on the investigation, an officer decides whether to forward a complaint that results in "petitioning" the juvenile court for a hearing. Individual juvenile arrest records are maintained locally, they are not consolidated to form any statewide, central law enforcement database.

The SBI's Division of Criminal Information (DCI) collects juvenile arrest data, excluding offender names, from law enforcement agencies through the national UCR Program. DCI provides statistical data about juvenile trends based on these arrests. Due to the fact that the UCR Program is voluntary and because of the nature of juvenile crime, these trends may not be representative of the total statewide experience.

Administrative Office of the Courts

Juvenile court counselors maintain involvement with a juvenile through all aspects of the juvenile justice system. They are responsible for making several decisions and critical recommendations about a juvenile offender. They must review, collect, summarize, and/or forward the core information regarding each juvenile offender processed through the juvenile court system. At some point they come in contact with the police report, juvenile petition, intake card, offender background (family, medical history, education, etc.), disposition, probation records, DYS release conference information, and aftercare reports. The juvenile court counselor is the only position in the system that routinely interfaces with everyone else involved in the juvenile justice process: police, clerk of the court, judge, DYS staff, and community agencies.

The information collected by juvenile court counselors is primarily a paper process. Some individual courts have automated selected records. Case records are court-based and not available through any statewide database. Juvenile court counselors may begin dealing with a juvenile and have no knowledge of an existing file in another jurisdiction. The counselors depend upon the juvenile or the parents to reveal any previous juvenile offenses in other jurisdictions. A court dealing with a new arrest requests existing juvenile offender information from any previous court jurisdiction identified by the parties. This manual system is time consuming and requires duplicate data entry by the law enforcement officer, juvenile court counselor, clerk of the court, and in some cases DYS. Duplicate data entry increases the likelihood of error. Some past juvenile offenses may not be identified by police or the juvenile court counselor if the offenses occurred in another jurisdiction.

If a petition is deemed appropriate, the juvenile court counselor forwards petition information to the clerk of the court. The clerk is responsible for the formal petition. In the ideal situation, a law enforcement officer takes the initiative to complete the juvenile petition satisfactorily which reduces the work required by the juvenile court counselor and the clerk of the court. The petition can then be reviewed, forwarded and recorded appropriately. The clerk of the court is also responsible for scheduling the hearing and issuing a summons to the juvenile.

The juvenile court counselor collects juvenile background information for the judge before disposition. At times counselors have difficulty collecting medical and educational records. The school or medical facility may raise an issue of confidentiality and refuse to comply in a timely fashion. In these cases, if the juvenile is to be committed, it is left to DYS to collect a copy of these records after commitment. The format for summarizing and presenting juvenile background information to the judge varies. Juvenile judges expressed concern that they receive inadequate information from juvenile court counselors. Inadequate information may result from a decentralized manual information system, inconsistent report formats, and inconsistent standards across the state.

Disposition information is entered for the state by the clerk and at the local court level by the juvenile court counselor. If a juvenile is placed on probation, the offender records are readily accessible to the juvenile court counselor assigned the case. If the juvenile is committed to the DYS, the juvenile court counselor notifies DYS as soon as possible. The counselor is also responsible for identifying relevant information from the case file and forwarding it with the juvenile upon commitment to DYS. DYS cites times when they did not receive adequate information from the juvenile court counselors. This may be due to:

- inconsistent formats and standards across courts
- information being withheld by schools, medical professionals, or others
- the practice of forwarding information in a summary format instead of providing original documents
- a change in the process that mandates a juvenile be physically transferred to DYS as soon as possible after the commitment order.

Juveniles used to be placed in detention for a short period while juvenile court counselors completed collecting and summarizing information for DYS. This practice ended abruptly because of a lawsuit predicated on overcrowding. Because of this court counselors had to commit juveniles to DYS prior to having all information available. AOC Juvenile Service's staff suggests that counselors have since adjusted and all available information is again accompanying juveniles to DYS.

DYS and the juvenile court counselor hold an aftercare conference before releasing a juvenile. Once the juvenile is released and under the supervision of the counselor, DYS does not receive any information. The previous DYS Director asked AOC to discontinue exchanging aftercare information. AOC Juvenile Services expressed a willingness to provide this information again if requested by the current DYS Director.

As stated, individual courts do not forward offender names or specific case information to any central case history database. However, individual courts do forward summary data to AOC, Juvenile Services. This allows AOC to summarize aggregate data about juvenile court cases across the state.

Division of Youth Services

According to DYS, comprehensive juvenile background information may or may not be passed to them when a juvenile is adjudicated delinquent and committed to their facilities. Even if the collected information is passed to DYS it may not be as thoroughly documented as needed for evaluating the various needs of the juvenile. Thorough, timely juvenile background information is a critical need for DYS.

DYS maintains databases that are event based, and tracks admission and release from detention facilities, training schools, camps and community based alternative programs**.** There are three hundred and ninety-nine community based alternative programs. Each program submits a hard copy of admission and release data quarterly. DYS then enters the information into their computer system. DYS facilities do not have an automated on-line system to share information within the agency.

DYS does not receive aftercare information from juvenile court counselors nor adult recidivism data from the Department of Correction. This lack of feedback inhibits efforts to evaluate the effectiveness of individual intervention strategies, as well as, the system as a whole.

The state of the DYS information system is addressed in their Annual Information System Plan for fiscal year 1994-1995. DYS is experiencing an increased demand for services with an antiquated information system.

> "... With the ever increasing demand to serve more children in all our programs, especially secure detention and training school, we are being asked to provide information on a moment's notice in volumes and formats that require a broad range of automation strategies. Our detention centers and training schools are consistently above capacity, our community based programs, Eckerd camp programs, and non-secure programs are having to expand services far beyond previous expectations.
>
> These pressing issues, alone with the need to provide our users with the basic tools for information gathering and distribution, have prompted an all-out effort by the Division to upgrade hardware, software, mainframe programs, and, indeed, to assess the entire automation process. We foresee the need to provide common data entry screens, edit functionality that will prevent corrupt data from entering the system, and, above all, a system that will provide management with the data necessary to make informed decisions as well as provide pertinent information for the state legislature, and other criminal justice agencies. It is essential that we provide to the extent possible, the capacity to measure effectiveness of DYS programs, including education, treatment, and placement."

Since this report, DYS has continued to improve their systems. They are working with the Department of Human Resources to move DYS to a LAN environment. There is an initiative to develop a statewide, automated Welfare Information System. DYS is meeting with the Division of Social Services and Division of Mental Health to determine what role, if any, DYS will have in that system. There is federal money available for such an effort.

Interagency Issues

Juvenile justice agencies share common information needs when processing a juvenile case. Most agencies need to know identification and demographic information, such as, name, age, birth date, parent / guardian, etc. There are duplicate data collection and recording efforts by juvenile court counselors, clerks, detention facilities, DYS central

office, and individual training schools. This duplication wastes personnel time and increases the potential error rate with every entry into the system. Much of the data entry about juvenile offenders is completed manually which is very time consuming and difficult to retrieve by others who need the information.

Court counselors, judges, and DYS staff need thorough background information. The current lack of agency automation and interagency interfaces create difficulty in accessing and retrieving needed information. It also leads to inconsistent information at various decision points in the process.

Agencies are searching for strategies to effectively deter and rehabilitate the juvenile offender. The current environment does not support the type of research needed to make informed decisions. The DCI system for analyzing juvenile crime is based upon inconsistent reporting by law enforcement agencies. Because this system is not offender based and only analyzes juvenile arrests report for UCR purposes it is not necessarily a useful tool in which to measure the effectiveness of juvenile treatment. The AOC system for analyzing juvenile trends is also not offender-based. It uses only aggregate data and cannot measure the effectiveness of juvenile treatment. Researching recidivism within the state is difficult without an automated master name index linking all juvenile offense events. Currently, a juvenile's name may be listed differently in differing jurisdictions. Recidivism research also requires the ability to search juvenile and adult databases. There is no ability to retrieve admission data from DOC.

Approach

- Review the need for access to juvenile data
- Conduct an audit of juvenile court counselor case files
- Automate and interface information systems
- Establish reliable, automated, statewide databases

Review the need for access to juvenile data

The CJIN governance structure should review the current laws governing access to juvenile offender records and determine if additional access should be granted to criminal justice professionals. Additional access will require a change of state law.

Conduct an audit of juvenile court counselor case files

AOC should conduct an audit of juvenile court counselor case files. The audit will examine the:

- level and consistency of detail in juvenile information collected, summarized, and forwarded to judges and other professionals charged with court ordered juvenile supervision.

- degree of standardization of reporting formats used across court jurisdictions.

Sample case files modeling the formats and standards desired for all courts should be used in the training. A system for random sampling across all courts should be calculated and team members assigned to review files selected based on the random system. Team auditors should review files and document their level of compliance with the desired formats and standards. Common areas of file deficiencies should be noted for later training purposes.

Automate and Interface Information Systems

The AOC, Juvenile Services should coordinate a statewide effort to develop an automated juvenile case records system. They can leverage efforts already underway by courts that have identified common data elements and automated selected databases. AOC Juvenile Services should automate for the information needs of the juvenile court counselor, clerk of the court, and judge. They should also consider information needs that detention facilities, camps, and training schools have from AOC and design the system to interface with DYS.

Both AOC and DYS automation efforts must be compatible with the adult CJIN component. Interfaces should be established between the AOC, DCI, DOC, and DYS. These interfaces will eliminate duplication of data entry, generate reports based on aggregate data, and facilitate research on the effectiveness of juvenile treatment. Only authorized users will be given access to information.

Establish reliable, automated, statewide databases

Establish a Statewide Identification Index of juveniles which flags any item requiring immediate attention, such as, runaway status, subject demographic information, and other offense information. Also establish a single, statewide, juvenile personal identification number to link a juvenile's record of arrests, court cases, dispositions, probation, custody, aftercare, and release data. When juvenile offenders commit their first adult crimes, each individual will receive a new adult identifier. The juvenile identification number and the adult identification number can be linked in the databases. The state should consider fingerprinting juveniles who are adjudicated delinquent and committed to DYS. This will begin to establish a database for positive identification. It will be especially helpful when tracking individuals across the juvenile and adult correction systems.

This will give North Carolina statewide, automated databases, easily accessible to those in the juvenile system who are trying to make decisions about an individual juvenile's welfare or about the system itself. The suggestion of statewide juvenile databases raises a fear among some juvenile justice professionals that information will be misused. They fear that
confidential information will be accessed by a nonauthorized user or that a newly authorized user will misuse information when dealing with a juvenile.

Initial Cost Estimates

AOC Automation

Cost Components	Internal Development ($)	Leveraged Implementation ($)
Hardware and Database[1]	5,300,000	5,300,000
Software Development / License	1,386,000	1,000,000
Source Code	na	1,000,000
Initial Training	110,000	110,000
File Audit / Analysis[2]	528,000	528,000
Business Process Analysis[3]	396,000	396,000
Project Management[4]	528,000	528,000
Total	**$8,248,000**	**$8,862,000**

[1] Costs for hardware, software development, software license, source code and training were extrapolated from internal AOC cost estimates.

[2] Four teams of two auditors for a period of approximately 3 months at an average monthly cost $22,000.

[3] Assumes three full time equivalents for six months at an average FTE cost of $22,000 per month.

[4] Project management assumes 2 FTEs for one year.

Ongoing Cost Estimates

Cost Component	Internal Development (Annual $)	Leveraged Implementation (Annual
Maintenance[5]	$876,500	$780,000
Training [6]	$264,000	$264,000
Total	**$1,140,500**	**$1,044,000**

[5] 25% of the software development cost, and 10% of the combined hardware and database costs.

[6] Training costs include 1 full-time trainer for a period of one year at an average cost of $22,000 per month.

Implementation Alternatives

The project team identified three alternative implementation strategies to achieve the single vision of an integrated criminal justice information network. This section presents these implementation and cost alternatives. Even though the same critical projects are recommended with each alternative, variations in timing provide the state of North Carolina flexibility in achieving implementation objectives.

The three implementation alternatives for the recommended CJIN projects span a five-year period, with the exception of the Mobile Voice and Data project, which spans a ten-year period.

The Governance Board, Data Sharing Standards Development project (1), and the CJIN Security project (2), have the same timeframes, regardless of the alternative selected. The TCP/IP project (3), and the End-User Technology Upgrade project (4), are phased in to correspond with the pace of the projects they support.

The Statewide Mobile Voice and Data project (5) costs are presented in a separate table at the end of this section.

The first alternative assumes staggered two-year time-frames for implementing projects 6 through 12.

The second alternative assumes development of projects 6 through 12 over a four-year timeframe, with projects beginning in either year one or year two.

The third alternative assumes a combination of two to five-year timeframes for implementing projects 6 through 12 starting in various years, which allows both the purchase of commercially available software and custom development.

Although extending the time period over which the recommended projects are implemented will reduce the costs in the

first few years, stretching the timeline will increase the overall costs to the state. There will be delays in the benefits documented within this study. In addition, delays in implementation will cause some state and local jurisdictions to further commit their limited funds to the development of systems that do not necessarily support a statewide, integrated network.

When a project has been implemented over multiple years, the ongoing (or yearly) costs have been prorated according to the portion of the project implemented in each year. For example, in alternative one, the Statewide Magistrate System project will be implemented over two years. The ongoing yearly costs for the first year of implementation is $0.7 million, or one-half of the total expected yearly support costs. When the Magistrate system is fully implemented, ongoing yearly support costs will be the full $1.3 million.

Key implementation milestones have been indicated by the "milestone marker" (▼). This symbol is used to indicate the completion of an important phase within the overall CJIN strategy that should result in the greatest gains in efficiency and information availability based on the synergy of one or more projects.

Cost information is provided only as an indicator of potential project scope and should be used as a basis for long-term planning. Subsequent budget estimates should be based on prevailing market prices at the time the work is to be undertaken and adjusted by the final scope of the work. Complete project descriptions, estimated costs detail, and costing assumptions are contained within Section VI - Overview of CJIN Projects.

Summary of Estimated Costs for Recommended CJIN Projects

The following table provides a summary of the total estimated initial and ongoing costs for each recommend project.

Project Costs ($millions)	*Initial Costs*	*Annual Costs*
Governance Board	$0.4	$0.7
1. Data Sharing Standards Development ▼	$2.1	$0.8
2. CJIN Security	$0.9	$0.1
3. TCP/IP	$4.6	$13.9
4. End-User Technology Upgrade	$21.2	$1.9
5. Statewide Mobile Voice and Data (separate table)	***	***
6. Statewide Automated Fingerprint Identification System ▼	$22.4	$2.6
7. Statewide Magistrate System ▼	$5.0	$1.3
8. Statewide Identification Index	$6.7	$1.4
9. Statewide Criminal History Repository	$4.8	$1.0
10. Statewide Warrant Repository	$4.2	$1.1
11. Courtroom Automation ▼	$10.1	$2.0
12. Juvenile Records Automation	$8.8	$1.1

Project Costs ($millions)	*Initial Costs*	*Annual Costs*
Totals	**$91.2**	**$27.9**

▼ - Milestone marker - see explanation at the front of this section.

Implementation Alternative 1

The Governance Board, Data Sharing Standards Development project (1), and the CJIN Security project (2), have the same timeframes regardless of the alternative selected. The TCP/IP project (3), and End-User Technology Upgrade project (4), are phased in to correspond with the pace of the projects they support.

The Statewide Mobile Voice and Data project (5) costs are presented in a separate table at the end of this section.

This first alternative assumes staggered two-year time-frames for implementing projects 6 through 12. By concentrating resources in this manner, CJIN will have fewer simultaneous projects. Further, projects will have firm deadlines for development, distribution, and implementation. The reduced timeframe in many cases rules out the ability to develop software in-house.

Alternative 1

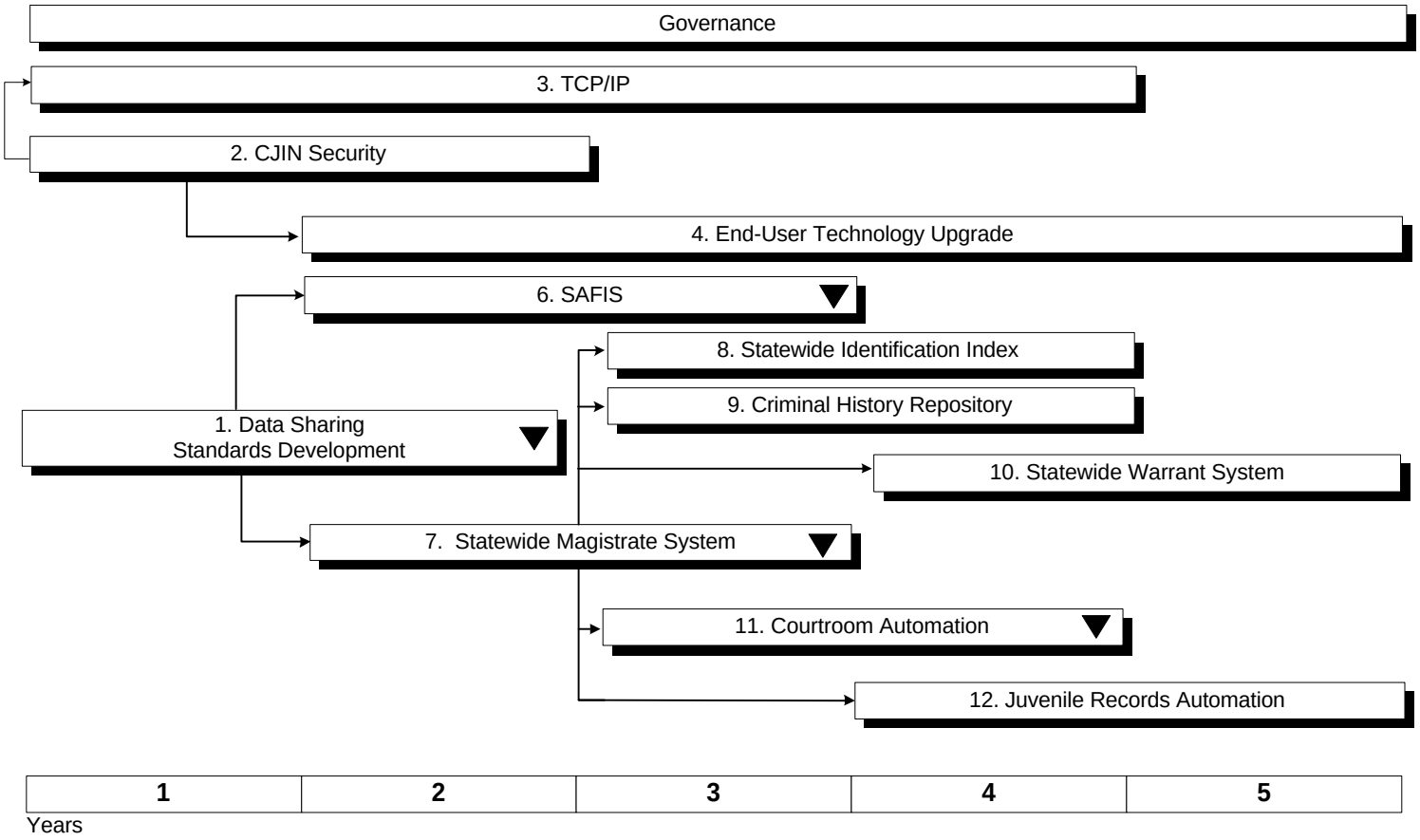


Figure VII-1

Alternative 1: Projects Implemented in Two-Year Timeframes ($millions)											
Project	**Yr. 1**		**Yr. 2**		**Yr. 3**		**Yr. 4**		**Yr. 5**		**Total**
	Init	Yrly	Init	Yrly	Init	Yrly	Init	Yrly	Init	Yrly	
Governance Board	0.4			0.5		0.7		0.7		0.7	$3.0
1. Data Sharing Standards	1.0		1.1			0.8		0.8		0.8	$4.5
2. CJIN Security	0.4		0.5			0.1		0.1		0.1	$1.2
3. TCP/IP	1.1		1.1	3.5	1.2	7.0	1.2	10.5		13.9	$39.5
4. End-User Technology Upgrade			5.3	0.5	5.3	1.0	5.3	1.5	5.3	1.9	$26.1
5. Mobile Voice and Data (separate table)											
6. SAFIS			11.2	1.3	11.2	2.6		2.6		2.6	$31.5
7. Statewide Magistrate System			2.5	0.7	2.5	1.3		1.3		1.3	$9.6
8. Statewide Identification Index					3.3	0.7	3.4	1.4		1.4	$10.2
9. Statewide Criminal History Repository					2.4	0.5	2.4	1.0		1.0	$7.3
10. Statewide Warrant Repository							2.1	0.5	2.1	1.1	$5.8
11. Courtroom Automation					5.0	1.0	5.1	2.0		2.0	$15.1

Alternative 1: Projects Implemented in Two-Year Timeframes ($millions)											
12. Juvenile Records Automation							4.4	0.5	4.4	1.1	$10.4
Annual Totals	**$2.9**	**$0.0**	**$21.7**	**$6.5**	**$30.9**	**$15.7**	**$23.9**	**$22.9**	**$11.8**	**$27.9**	**$164.2**

Implementation Alternative 2

The Governance Board, Data Sharing Standards Development project (1), and the CJIN Security project (2), have the same timeframes regardless of the alternative selected. The TCP/IP project (3), and End-User Technology Upgrade project (4), are phased in to correspond with the pace of the projects they support.

The Statewide Mobile Voice and Data project (5) costs are presented in a separate table at the end of this section.

This second alternative assumes development of projects 6 through 12 over a four-year timeframe, with projects beginning in either year one or year two. This approach will accommodate software development schedules and controlled distribution and implementation roll-outs.

Alternative 2

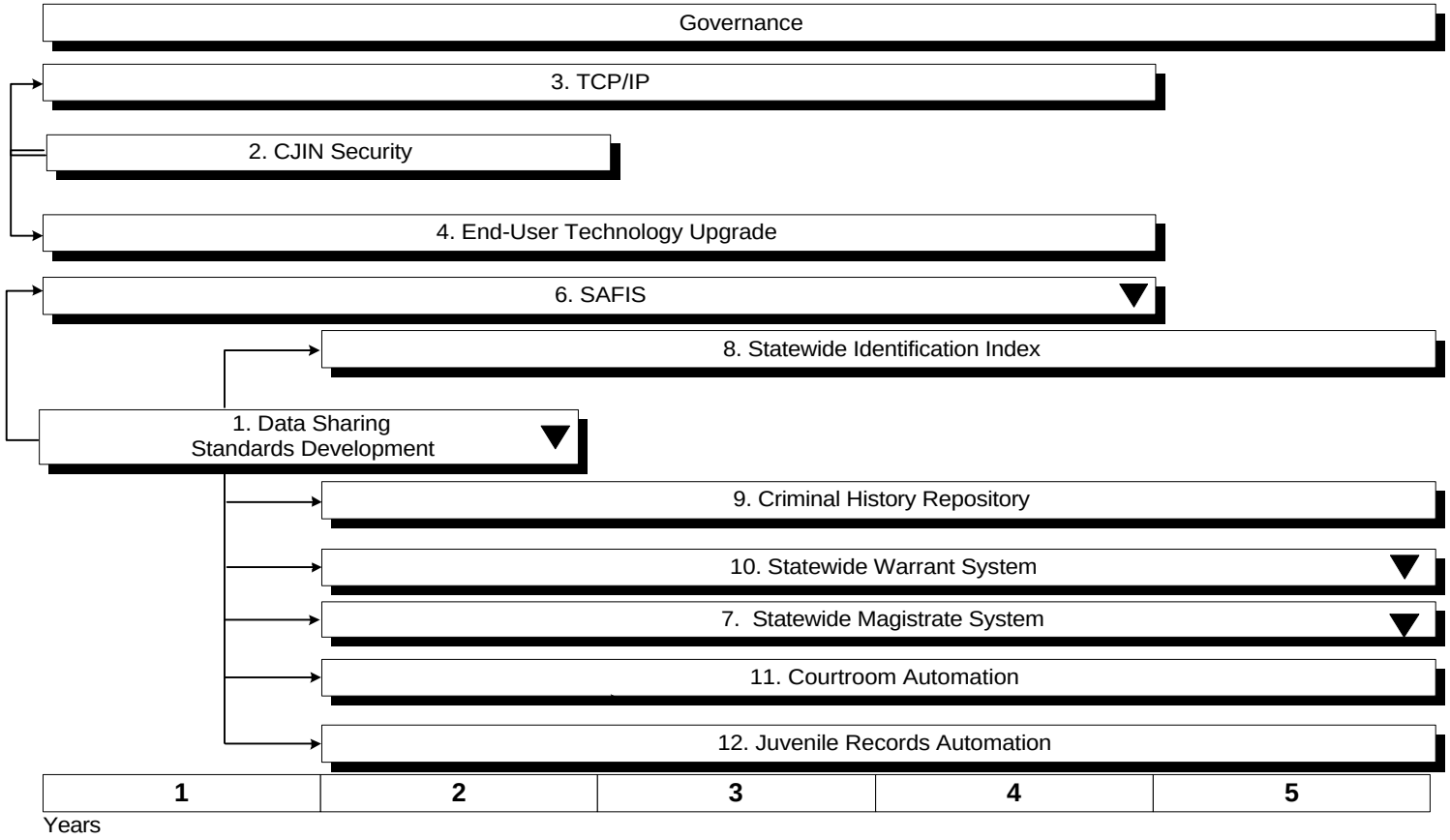


Figure VII-2

Alternative 2: Projects Implemented in Four-Year Timeframes ($millions)											
Project	**Yr. 1**		**Yr. 2**		**Yr. 3**		**Yr. 4**		**Yr. 5**		**Total**
	Init	Yrly	Init	Yrly	Init	Yrly	Init	Yrly	Init	Yrly	
Governance Board	0.4			0.5		0.7		0.7		0.7	$3.0
1. Data Sharing Standards	1.0		1.1			0.8		0.8		0.8	$4.5
2. CJIN Security	0.4		0.5			0.1		0.1		0.1	$1.2
3. TCP/IP	1.1		1.1	3.5	1.2	7.0	1.2	10.5		13.9	$39.5
4. End-User Technology Upgrade	5.3	0.5	5.3	1.0	5.3	1.5	5.3	1.9		1.9	$28.0
5. Mobile Voice and Data (separate table)											
6. SAFIS	5.6	0.6	5.6	1.3	5.6	1.9	5.6	2.6		2.6	$31.4
7. Statewide Magistrate System			1.2	0.3	1.3	0.7	1.2	1.0	1.3	1.3	$8.3
8. Statewide Identification Index			1.6	0.3	1.7	0.7	1.7	1.0	1.7	1.4	$10.1
9. Statewide Criminal History Repository			1.2	0.2	1.2	0.5	1.2	0.7	1.2	1.0	$7.2
10. Statewide Warrant Repository			1.0	0.3	1.0	0.6	1.1	0.9	1.1	1.1	$7.1
11. Courtroom Automation			2.5	0.5	2.5	1.0	2.5	1.5	2.6	2.0	$15.1

Alternative 2: Projects Implemented in Four-Year Timeframes ($millions)											
12. Juvenile Records Automation			2.2	0.3	2.2	0.6	2.2	0.9	2.2	1.1	$11.7
Annual Totals	**$13.8**	**$1.1**	**$23.3**	**$8.2**	**$22.0**	**$16.1**	**$22.0**	**$22.6**	**$10.1**	**$27.9**	**$167.1**

Implementation Alternative 3

The Governance Board, Data Sharing Standards Development project (1), and the CJIN Security project (2), have the same timeframes regardless of the alternative selected. The TCP/IP project (3), and End-User Technology Upgrade project (4), are phased in to correspond with the pace of the projects they support.

The Statewide Mobile Voice and Data project (5) costs are presented in a separate table at the end of this section.

This third alternative assumes a combination of two to five-year timeframes for implementing projects 6 through 12, which allows both the purchase of commercially available software and custom development.

Alternative 3

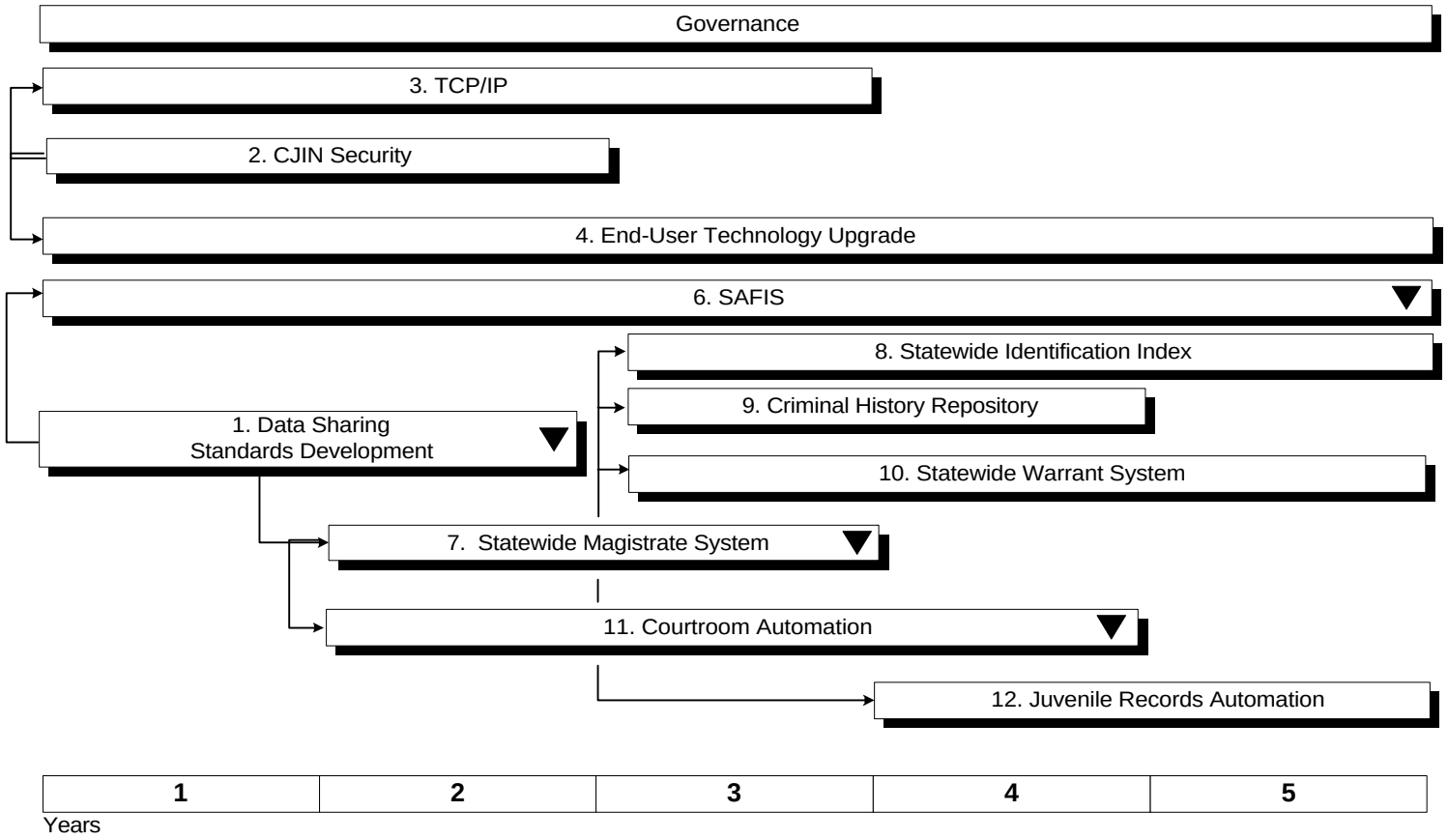


Figure VII-3

Alternative 3: Projects Implemented in Two to Five Year Timeframes ($millions)											
Project	**Yr. 1**		**Yr. 2**		**Yr. 3**		**Yr. 4**		**Yr. 5**		**Total**
	Init	Yrly	Init	Yrly	Init	Yrly	Init	Yrly	Init	Yrly	
Governance Board	0.4			0.5		0.7		0.7		0.7	$3.0
1. Data Sharing Standards	1.0		1.1			0.8		0.8		0.8	$4.5
2. CJIN Security	0.4		0.5			0.1		0.1		0.1	$1.2
3. TCP/IP	1.1		1.1	3.5	1.2	7.0	1.2	10.5		13.9	$39.5
4. End-User Technology Upgrade	4.2	0.3	4.2	0.7	4.2	1.1	4.3	1.5	4.3	1.9	$26.7
5. Mobile Voice and Data (separate table)											
6. SAFIS	4.4	0.5	4.5	1.0	4.5	1.5	4.5	2.0	4.5	2.6	$30.0
7. Statewide Magistrate System			2.5	0.7	2.5	1.3		1.3		1.3	$9.6
8. Statewide Identification Index					2.2	0.4	2.2	0.9	2.3	1.4	$9.4
9. Statewide Criminal History Repository					2.4	0.5	2.4	1.0		1.0	$7.3
10. Statewide Warrant Repository					1.4	0.3	1.4	0.7	1.4	1.1	$6.3
11. Courtroom Automation			3.3	0.6	3.4	1.3	3.4	2.0		2.0	$16.0

Alternative 3: Projects Implemented in Two to Five Year Timeframes ($millions)											
12. Juvenile Records Automation							4.4	0.5	4.4	1.1	$10.4
Annual Totals	**$11.5**	**$0.8**	**$17.2**	**$7.0**	**$21.8**	**$15.0**	**$23.8**	**$22.0**	**$16.9**	**$27.9**	**$163.9**

CJIN Governance Board Costs

The following table provides the estimated staffing and administrative costs for related the CJIN Governance Board. All figures include fringe benefits of 27% and an annual cost-of-living increase of 4% for years two through five.

CJIN Governance Board Costs ($)					
Cost Category	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
Executive Director ($100,000 base)	127,000	132,080	137,363	142,858	148,571
Administrative Assistant ($30,000 base)	38,100	39,624	41,209	42,857	44,572
Secretary ($22,000 base)	27,940	29,058	30,220	31,428	32,686
Technical Staff ($60,000 base) 2 staff in year 1, 4 staff in year 2, 5 staff in years 3 to 5	152,400	316,992	412,090	428,574	445,717
Office Furniture, Computers/Printers, Copier and Supplies	15,000	4,000	2,000	2,000	2,000
Travel Expenses	7,000	10,000	12,000	12,000	12,000
Rental Space (1,200 square feet @ $12 per square foot)	14,400	14,400	14,400	14,400	14,400
Totals	**$381,840**	**$546,154**	**$649,282**	**$674,117**	**$699,946**

Statewide Mobile Voice and Data Implementation Costs

The following cost model for the statewide mobile voice and data project is based on the Michigan model where no payments are made to the vendor until the first phase has been accepted. Upon acceptance, a bulk payment is made and from then on progress payments are made each year. The table below projects state costs only and does not reflect local agency investments for portables, in-building coverage, and roaming stock.

Statewide Mobile Voice and Data Project - Projected State Cost ($Millions)											
Task\Year	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
MODAP Pilot	0.5	0.5	0.5								1.5
Frequency Study	0.5										0.5
County Planning	1.0	1.5	1.0	1.0	0.5	0.5	0.5	0.5	0.5	0.5	7.5
Implementation				35.0	35.0	35.0	34.0	34.0	34.0	34.0	241.0
Maintenance					3.5	6.0	8.5	13.5	16.0	18.5	66.0
Total ($millions)	**$2.0**	**$2.0**	**$1.5**	**$36.0**	**$39.0**	**$41.5**	**$43.0**	**$48.0**	**$50.5**	**$53.0**	**$316.5**